Court Services and Offender Supervision Agency (CSOSA)

Kiosk

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. CSOSA has documented contact and supervision standards, which include the frequency of office visits, employment verifications, home visits, and home verifications, which must be completed by the Community Supervision Officer with the offender throughout the period of supervision. Contact and supervision standards vary depending on the assessed level of risk the offender poses to the community (the higher the risk, the more frequent the contact).

The use of kiosks at CSOSA allows offenders who pose a very low level of risk to the community to use self-service technology to provide the information needed for the offender to fulfill his/her reporting requirement to CSOSA, and allow the Community Supervision Officer to meet the documented contact and supervision standards. The use of the kiosk self-service technology allows the offender to meet his/her office visit requirement. The personally identifiable information confirmed/provided by the offender through the kiosk self-service technology (residence, employment information, school information, emergency contact information) allows the Community Supervision Officer to complete the required verifications and meet the documented contact and supervision standards.

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

Information maintained in the kiosk 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.

CSOSA Operational Instruction CSS-2011-02 provides guidance on the supervision of cases assessed at a minimum level of risk, including the types of information used. CSOSA Operational Instruction CSS-2008-05 provides guidance on kiosk reporting, including the data to be collected from the offender.

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 approved to report through the kiosk self-service technology can only view, review, and update their own information. Offenders cannot search the information or search for information on other offenders who might be reporting through the kiosk self-service technology.

CSOSA staff members are able to search and retrieve the information by a number of personal identifiers: Last Name, First Name, Date of Birth, Police Department Identification (PDID), Probationer Identification (PIN), or CSOSA Number. At this time, the Privacy Act System of Records Notice being used for the kiosk system is the SMART (CSOSA's case management system) System of Records Notice. This Privacy Impact Assessment was requested to provide the documentation to review the status of the kiosk 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. 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 or to update the existing schedule (should there be one). 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 kiosk self-service technology are:

- Kiosk Incentive Behavior Contract: This form explains the compliance required by the offender to be able to report through kiosk self-service technology, and indicates what non-compliant behavior is and the ramifications of non-compliant behavior.
- Kiosk Enrollment Receipt: At the time the offender is enrolled to report through kiosk self-service technology, the offender is given a receipt with his/her PIN, the answers to the challenge questions, and general information about using the kiosk self-service technology and what to do if the offender encounters issues.
- Kiosk Receipt: Each time an offender reports through the kiosk self-service technology, he/she receives a paper receipt to document the completion of the reporting event.

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 Community Supervision Services provides each offender who is approved for reporting through the kiosk self-service technology with an orientation to the program and technology, including the ramifications of non-compliant behavior. CSOSA Office of Information Technology will work with CSOSA Community Supervision Services and CSOSA Office of General Counsel to review the materials used at orientation, and confirm and/or enhance the materials 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.

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.

The kiosk database, including personally identifiable information about the offender, is initially populated from staging tables which contain up-to-date information from CSOSA's case management system. All offenders should be aware of the information in CSOSA's case management system as the offender would have been responsible for providing much of the information to the Community Supervision Officer.

When the offender is enrolled in the kiosk program and participates in orientation, the initial information in the kiosk system will be the information received from the staging tables. At enrollment, the offender has the option to review the information with the Community Supervision Officer and notify the Community Supervision Officer of any issues or discrepancies. At that time, the offender will be given notice about the personal information collected from them while reporting through the kiosk self-service technology. CSOSA Office of Information Technology will work with CSOSA Community Supervision Services and CSOSA Office of General Counsel to review the materials used at orientation, and confirm and/or enhance the materials 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.

Kiosk Enrollment Receipt (printed at enrollment): CSOSA Office of Information Technology is currently working with CSOSA Office of General Counsel to review the Kiosk Enrollment Receipt provided to each offender, and enhance the receipt with a privacy statement which re-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.

During orientation and through the Kiosk 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 kiosk system is not shared directly from the kiosk system and not available for review by CSOSA staff members except those with access to the kiosk system. 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 not report in person, changes to the kiosk self-service technology, information that is to be collected, or information that is to be shared would need to be communicated by letter to each offender's residence address on record in the kiosk database. CSOSA Office of Information Technology will work with CSOSA Community Supervision Services to establish a process and procedures for flagging when these offenders need to be informed of changes to collected information, or when, how, why or under what circumstances collected information is shared.

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 kiosk system is information about the offenders who are approved for reporting through the kiosk self-service technology. This is a small sub-set of the entire offender population supervised by CSOSA.

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

3.2 What PII will the system include?

When an offender is initially enrolled for kiosk reporting, existing data on the offender is pulled into the kiosk database from a staging database/staging tables associated with CSOSA's case management system. This information consists of the following on each approved offender:

- last name
- first name
- date of birth
- Police Department Identification (PDID)
- CSOSA Number
- full term date (date when the offender's supervision expires)
- home address
- offender email
- home phone
- cell phone
- photo (due to the size of the photos, the photo is obtained as a view from the staging database/staging tables associated with CSOSA's case management system and not stored in the kiosk database)
- sex
- eye color
- hair color
- ethnicity
- race
- height
- weight
- employment information
- emergency (collateral) contact
- current assigned Community Supervision Officer

Once enrolled, the kiosk application adds information to the kiosk database, and CSOSA staff members who are authorized to access the kiosk system also add information to the kiosk database. That information includes:

- The Probationer ID (PIN) which is the key identifier used in the kiosk system to link all of the offender's information together. The kiosk system generates the PIN.
- A hand biometric scan. Hand biometric scanning is used in conjunction with the PIN for the offender to properly identify him or herself to the kiosk self-service technology. CSOSA staff members are also able to re-capture/redo the offender's biometric hand scan.
- Random selection for drug testing. The system generates and maintains a list of offenders who are selected to report for the use of illegal substances testing. When the offender reports, he/she is notified that he/she has been selected for drug testing and needs to report to one of CSOSA's Illegal Substance Collection Units.

Through the kiosk, the offender maintains his/her:

- home address, home phone and cell phone information
- employment information
- school and/or training information
- emergency contact information
- must report if he/she has been rearrested

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

- Logon information (username)
- Assigned role/permission level in the kiosk 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 kiosk system and kiosk self-service technology is necessary to achieve a number of purposes:

- The existing information pulled in from staging database/staging tables associated with CSOSA's case management system (e.g., name, date of birth, CSOSA Number, physical description) is used by CSOSA staff members to accurately identify the offender when he/she appears for enrollment in the kiosk system, and to confirm the approved offender is being enrolled.
- The Probationer ID (PIN) is generated by the kiosk system. The PIN, in conjunction with the hand biometric scan, allows the offender to properly identify him or herself to the

kiosk self-service technology, and enables the kiosk self-service technology to display the correct offender information for review and confirmation.

- The existing information pulled in from staging database/staging tables associated with CSOSA's case management system is also used to initially populate the kiosk self-service technology with the information that will be confirmed and updated by the offender when he/she appears for reporting.
- The personally identifiable information confirmed/provided by the offender through the kiosk self-service technology (residence, employment information, school information, emergency contact information) allows the Community Supervision Officer to complete the required verifications and meet the documented contact and supervision standards. This same information would be confirmed/verified if the offender were meeting with his/her Community Supervision Officer in person.
- All offenders under CSOSA supervision are subject to drug testing, including the sub-set of offenders approved for reporting through the kiosk self-service technology. The use of random selection for drug testing by the system provides a continued deterrent from drug and/or substance abuse by this sub-set of offenders, as well as early detection of substance abuse issues so that proper interventions can be put in place.
- The personally identifiable information on the CSOSA staff members is used to verify and validate that appropriate individuals are given access to the kiosk 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 kiosk 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 kiosk system (e.g., the PIN), or entered by CSOSA staff members into the kiosk system (e.g., by-pass flag). The data that is pulled 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 kiosk system includes:

- The Probationer ID (PIN). The kiosk system generates the PIN.
- A hand biometric scan.
- Random selection for drug testing.
- The information maintained by the offender throughout the reporting period of supervision (confirmations and changes to addresses, responses to the rearrest question, etc.).
- A record of successful and failed reporting attempts by the offender, including date reporting, time reporting, whether successful or failed, and kiosk used for reporting.
- Information added, updated and maintained by CSOSA staff members that supports on-going use of the kiosk self-service technology by the offender including:
  - Updates to any offender data in the kiosk system
  - Language preference: Whether the offender needs the screens and receipts to be in Spanish or English
  - A by-pass flag for the hand biometric scan

- A flag to indicate the offender's current reporting status through the kiosk self-service technology: Enabled, skip the next report, disabled.

Information maintenance and use: The information in the kiosk system is either maintained by the offender through the monthly reporting through the kiosk self-service technology (residence, employment, school and emergency contact information), or by CSOSA staff members who have access to the kiosk system. The Probationer ID/CSOSA # is used to link all of the information in the kiosk 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 kiosk system. In addition to allowing the offender to fulfill his/her reporting requirement to CSOSA, and allowing the Community Supervision Officer to meet the documented contact and supervision standards, the information in the kiosk system provides the basis for several reports (e.g., offenders who missed the assigned reporting window, offenders who failed to report, offenders who updated their information (and what piece of information), etc.).

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

Access to data by the offender is controlled through the use of the PIN, and the hand biometric scan. Entry of the PIN and a hand biometric scan are required every time the offender reports through the kiosk self-service technology. 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 kiosk system, his/her username and password are verified by Active Directory as being a successful match before access to the kiosk system is given. All CSOSA staff member access within the kiosk system is controlled by role. Roles define who can do what within the kiosk system. For example: Enter CSOSA numbers for approved eligible offenders, capture and re-capture the hand biometric, enroll the offender for reporting through the kiosk, monitor the kiosk machines, and give CSOSA staff members access to the kiosk system are all separate functions performed by CSOSA staff members in different roles within the kiosk system.

The kiosk system is in the process of meeting the federal requirements for system security. The Kiosk System Security Plan documents the system controls needed for the kiosk 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 kiosk system are those offenders who have been approved as eligible for reporting through the kiosk self-service technology, and have been enrolled into the kiosk system. For every offender report (each month), the kiosk system records and maintains successful and failed reporting attempts, including date reporting, time

reporting, whether successful or failed, and kiosk used for reporting. The system/database also maintains a history of each piece of information changed and/or updated by the offender. This provides the information needed by CSOSA staff members to verify and validate the offender's continued reporting, protects the offender by providing an auditable trail of all information maintained by the offender, and allows CSOSA staff to intervene if an offender appears to be having problems with the kiosk self-service technology.

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 kiosk self-service technology. CSOSA Office of Information Technology and CSOSA Office of General Counsel are working on an "offender" warning that will display when the offender logs into the kiosk self-service technology as an on-going reminder of the consent to provide the information, of CSOSA's uses of the information, and consent to being monitored. For the kiosk system, there are IIS logs (monitors accesses of the kiosk 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 kiosk 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 kiosk system or by whom, or there are questions about how information in the kiosk system was used by CSOSA staff members.

3.7 Will the system monitor employees or contractors?

The kiosk system/database maintains a history of each piece of information changed and/or updated by every CSOSA staff member who accesses the kiosk system.

Contractors do not have access to the kiosk 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 kiosk system from the CSOSA staff member view. All CSOSA staff members are made aware that accessing any system, including the kiosk system, constitutes agreement to be monitored through a warning that displays when he/she logs into the system. For the kiosk system, there are IIS logs (monitors accesses of the kiosk 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 (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 kiosk 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 kiosk system or by whom, or there are questions about how information in the kiosk 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 kiosk system and self service technology do 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 – no reports are available to offenders) through the CSOSA Portal (CSOSA staff view into CSOSA's Enterprise Data Warehouse) based on the data in the CSOSA Enterprise Data Warehouse. The alerts and reports made available through the CSOSA Portal for offenders who are reporting through the kiosk self-service technology include: Offenders who missed the assigned reporting window, offenders who failed to report, offenders who updated information (and what piece of information), offenders who report being re-arrested, etc. The information in the reports is not anonymized as the Community Supervision Officer needs to know which offender (e.g. failed to report, updated information, was re-arrested) 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 kiosk system relates to and supports one or more of the stated purposes. Offenders who are approved as eligible and enrolled in the kiosk system are made aware of the data they will be required to provide through the kiosk self-service technology and given the option to decline use of the self-service technology. If the offender does decline, he/she will continue to report to his/her Community Supervision Officer in-person.

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 kiosk system and kiosk self-service technology is limited to the personally identifiable information needed to meet the purposes of the kiosk system. The collected information allows the offender to meet his/her supervision reporting requirement by reporting on a set schedule (once per month during the week of his/her birth date), and collecting information specific to the verifications that need to be completed by CSOSA staff members to meet the documented contact and supervision standards (residence, employment information, school information, and emergency contact information).

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

- Policy: CSOSA Operational Instruction CSS-2011-02 provides guidance on the supervision of cases assessed at a minimum level of risk, including the types of information used, and the contact and supervision standards. CSOSA Operational Instruction CSS-2008-05 provides guidance on kiosk reporting, including the data to be collected from the offender, how often the offender is to report, when the reporting by-pass functionality is to be used, definition of non-compliant behaviors, and actions to be taken when an offender exhibits non-compliant behavior.
- Assignment of staff: In order to better support offenders reporting through the kiosk self-service technology, CSOSA has assigned all of the offenders reporting through the kiosk self-service technology to a limited number (currently 2) of Community Supervision Officers who only supervise offenders reporting through kiosk self-service technology. These Community Supervision Officers are held accountable to the verification, contact and supervision standards documented in CSOSA Operational Instruction CSS-2008-05. They are responsible for following up on offenders who fail to report as scheduled, verification of employment information maintained by offenders through the kiosk self-service technology, verification of changes to offender residence information, etc.
- Receipt: Each time an offender reports through the kiosk self-service technology, he/she receives a paper receipt to document the completion of the reporting event. The receipt indicates if the offender is required to report to his/her Community Supervision Officer to review and/or discuss any of the information maintained by the offender (e.g., a change to residence information would require the offender to provide some proof of the new residence – lease, mortgage document, electric bill, etc.) so that the Community Supervision Officer can perform the required employment, school and home

verifications.

- 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 reporting through the kiosk self-service technology are limited to the information available from the kiosk system. These alerts and reports relate the information entered by the offender through the kiosk self-service technology to the verifications and follow up actions that need to be completed by CSOSA staff members to meet the documented contact and supervision standards (residence, employment information, school information, and emergency contact information).

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 kiosk 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 (e.g., police requesting residence or employment addresses of an offender for legitimated law enforcement purposes), 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 kiosk system/database comes from one of four sources:

- The individual (offender): One of the main purposes of the kiosk self-service technology is to provide enrolled offenders with a mechanism for self maintenance of residence, employment, school and emergency contact information.
- From another CSOSA IT system: When an offender is enrolled for kiosk reporting, specific existing data on the offender is pulled into the kiosk database 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. This eliminates the need to manually enter the same information into the kiosk database (e.g., eliminates the possibility of manual data entry errors), provides the base demographic data needed by staff to properly identify the offender, and provides the initial residence, employment, school and emergency contact information that the offender will review, confirm and maintain via monthly reporting through the kiosk self-service technology.
- Generated by the kiosk system: While minimal, the kiosk system generates the Probationer ID, which is the key used throughout the kiosk system to link the

offender's information together regardless of the source of entry.

- Entered by CSOSA staff: CSOSA staff members are responsible for maintaining and updating the system settings for on-going use of the kiosk self-service technology by the offender. As time goes by, the offender's ability to use the kiosk self-service technology may change. The information entered by staff includes the capture of the hand biometric (offender's right hand), recapture of the hand biometric when needed, review of the data in the kiosk system to verify it is up-to-date and accurate, disabling an offender from reporting through the kiosk self-service technology (at the end of supervision, or due to non-compliance), and re-enabling and offender to report through the kiosk self-service technology.

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

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

The internal systems the kiosk system/database interacts with are:

- CSOSA's case management system:
  - Existing data on the offender is pulled into the kiosk database 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 approved eligible offender.
  - The information is read-only from the staging database/staging tables and is pulled into the kiosk system electronically. Photos are not pulled into the kiosk system. When access to the photo is needed, it is made available real-time via a read-only view from the staging database/staging tables.
  - 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 kiosk system, is read-only.
  - The Kiosk System Security Plan defines the system boundaries for the kiosk 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:
  - Reporting information from the offenders' use of the kiosk self-service technology is pulled electronically from the kiosk database into CSOSA's Enterprise Data Warehouse on a nightly basis. Information on offenders who successfully reported on time, successfully reported but outside the approved reporting window, failed to report, had issues reporting, and data modified/updated by the offender through the kiosk self-service technology are some of the reports available to CSOSA staff members through CSOSA's Enterprise Data Warehouse.
  - The information is read-only from the kiosk database and is pulled by CSOSA's Enterprise Data Warehouse.
  - The Kiosk System Security Plan defines the system boundaries for the kiosk 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, system security, and workstations needed by the kiosk 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 kiosk system.
  - The Kiosk System Security Plan defines the system boundaries for the kiosk 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 kiosk 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 what information he/she is responsible for maintaining, how often he/she is to report, what to do if he/she cannot report as scheduled, and that he/she is responsible for the accuracy and completeness of that information.
- From another CSOSA IT system: Following up with staff to make sure they take the time to validate the information pulled into the kiosk database 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 kiosk system/database with external parties, CSOSA staff members need to be reminded this includes the lookup and printing of data directly from the kiosk 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 for kiosk reporting, specific existing data on the offender is pulled into the kiosk database from a staging database/staging tables associated with CSOSA's case management system. The enrollment is done with the offender present due to the required in-person orientation for the offender. At the time of enrollment, the CSOSA staff member and the offender are able to review the data pulled into the kiosk database, and make updates and corrections, or make note of updates and corrections to be made in CSOSA's case management system and by IT staff.
- Generated by the kiosk system: Information generated by the kiosk 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.
- The individual (offender): Information supplied by the offender is verified by a CSOSA staff member who will take appropriate follow up action depending on the information updated by the offender. These actions include: Review of lease or mortgage documents, review of pay stubs, calls to employers and emergency contacts, review of school documents, and follow up calls with the appropriate law enforcement authorities regarding reports of re-arrests. If the information entered by the offender cannot be confirmed as accurate and complete, the CSOSA staff member conducting the follow up will enter the last known and confirmed information in the kiosk system.
- Entered by CSOSA staff: Supervisors are responsible for verifying CSOSA staff members (Community Supervision Officers in particular) are adhering to policy and entering accurate and complete data into the kiosk system. On an annual basis, a complete review of each offender's electronic and paper record is completed by the assigned Supervisor.

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 kiosk system, they uncover situations where data is incorrect, data cannot be updated, or the kiosk system does not perform

as designed. Some previous examples which have now been corrected include reporting windows that cross months, reporting while in an excused status, and switching between employed and unemployed. As issues are identified with the kiosk system, the issues are documented and investigated. If the issue is specific to that offender's data, the offender, 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 kiosk 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?

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

- Offender:
  - Access: Offenders who are approved for enrollment in the kiosk self-service technology will be able to review, confirm and/or update their residence, employment, school and emergency contact information through the self-service technology.
  - Process and authorization for access: The CSOSA Number of each approved eligible offender is manually entered into the kiosk system/database by a CSOSA staff member selected to perform this function. The offender is contacted about participation in the program, and an orientation appointment is set up. At the orientation, the offender is enrolled into the kiosk system, including capture of the hand biometric, and generation of a Probationer ID (PIN) by the kiosk system (if not already completed). Once the orientation and enrollment are complete, the offender may use the kiosk self-service technology.
  - Process and policies surrounding termination: CSOSA Operational Instruction CSS-2008-05 provides guidance on the kiosk program, including those behaviors or actions determined to be "non-compliant" and the resulting actions, which can be termination from use of the kiosk self-service technology. Offenders who are approaching the end of their period of supervision are terminated from kiosk reporting. Termination is accomplished by disabling the offender's ability to use the kiosk self-service technology (flag in the kiosk system is set to "disabled" by CSOSA staff members).
- Community Supervision Officer:
  - Access: Community Supervision Officers assigned to supervise offenders reporting through the kiosk self-service technology have access to all of the offender data in the kiosk application. They also have access to all of the kiosk-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 kiosk Business Analyst role to complete the account in the kiosk system, including the assignment of the kiosk 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 kiosk Business Analyst role would disable the kiosk system account.

- Supervisory Community Supervision Officer:
  - Access: All Community Supervision Officers are assigned to a Supervisory Community Supervision Officer. The Supervisory Community Supervision Officer has access to all information available to the Community Supervision Officers that are assigned. For the kiosk system, Supervisory Community Supervision Officers, to whom Community Supervision Officers responsible for supervising offenders reporting through the kiosk self-service technology are assigned, have access to all of the offender data in the kiosk application. They also have access to all of the kiosk-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 kiosk Business Analyst role to complete the account in the kiosk system, including the assignment of the kiosk 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 kiosk Business Analyst role would disable the kiosk system account.
- Branch Chief:
  - Access: Is similar to the Supervisory Community Supervision Officer: Access to all of the offender data in the kiosk application for assigned Community Supervision Officers/Supervisory Community Supervision Officers. They also have access to all of the kiosk-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 kiosk Business Analyst role to complete the account in the kiosk system, including the assignment of the kiosk 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 kiosk Business Analyst role would disable the kiosk system

account.

- Community Supervision Services – Management:
  - Access: Individuals within the management team within CSOSA Community Supervision Services would be given access to all of the kiosk-related data reports in the CSOSA Portal. In certain circumstances, selected individuals would be given access to the kiosk system.
  - 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 kiosk Business Analyst role to complete the account in the kiosk system, including the assignment of the kiosk 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 kiosk Business Analyst role would disable the kiosk 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 kiosk 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. To obtain 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 Server in order to develop the scripts needed to pull the data from the kiosk database in order to generate reports through CSOSA's Enterprise Data Warehouse/CSOSA Portal.
  - 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 kiosk application or database. Infrastructure is responsible for the servers and network on which the kiosk 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.

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

- Kiosk Attendant: Can enroll offenders for kiosk reporting (preferred language, challenge questions, by-pass flag, drug testing flag, and issue a receipt); monitor offender kiosk reporting; review offender data in the kiosk database; update the "by-pass" flag; update the drug testing flag; leave messages for offenders; and indicate if an offender is excused from reporting or disable an offender's reporting capability. CSOSA staff members with this role include Community Supervision Officers, Supervisory Community Supervision Officers, and Branch Chiefs with a need to access the kiosk system.
- Business Analysts: Can assign CSOSA staff members to the various roles in the kiosk system; edit CSOSA staff member information; maintain lookup values; add and edit messages by location; and set drug testing parameters. CSOSA staff members with this role would be selected and approved by the Associate Director, CSOSA Community Supervision Services and the Chief Information Officer.
- System Administrator: Can add or disable kiosk units; monitor kiosk units; and bring down or unresponsive units back on-line. CSOSA staff members with this role would be selected and approved by the Chief Information Officer.
- 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 kiosk, offender reporting problems, problems with the hand readers, etc. CSOSA staff members with this role would be selected and approved by the Associate Director, CSOSA Community Supervision Services and the Chief Information Officer.
- Eligible Offender Inputter: Can add eligible approved offenders to the kiosk database indicating the offender can be enrolled for reporting through the kiosk self-service

technology. CSOSA staff members with this role would be selected and approved by the Associate Director, CSOSA Community Supervision Services and CSOSA Office of the Director

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

The System Security Plan for the kiosk system 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 kiosk 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 kiosk system will be secured through the following controls:

- Physical controls:
  - Kiosk self-service technology (kiosk units) are located in the lobbies of four CSOSA offices staffed with Security Guards who are within 10 - 25 feet of the kiosk units.
  - The kiosk units are enclosed in locked metal enclosures with physical access limited to the touch screen monitor and the printer.
  - Lock boxes have been placed on the Local Area Network jacks and the power outlets to eliminate “inadvertent” unplugging of the units.
  - The kiosk application runs in “Kiosk” mode in Internet Explorer and the workstation account running the kiosk application is locked down to prohibit the workstation from being used for anything else should the application exit improperly.
  - 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.
- CSOSA does support remote access for CSOSA staff members (not offenders). Extra authentication in the form of a PIN and code from a token is required to authenticate to the network. Once a CSOSA staff member has successfully authenticated to the network, the kiosk application can be accessed if the CSOSA staff member is an authorized user of the kiosk system.
- The servers running the kiosk application, housing the kiosk 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 kiosk system run on the CSOSA network and are logically located behind the internal firewall.
  - The servers running the kiosk application, housing the kiosk 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 kiosk 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 kiosk database server and CSOSA's Enterprise Data Warehouse (server) in order to protect the kiosk 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 kiosk application is web-based to make it available on CSOSA's Intranet. All kiosk unit access to the kiosk application server is protected by a Secure Socket Layer (SSL) Certificate, which encrypts information between the kiosk unit and the kiosk application server.
  - CSOSA staff member access to the kiosk application server from their workstations is protected by the same Secure Socket Layer (SSL) Certificate.
  - The physical database on the kiosk database server is protected using transparent data encryption, which protects the data when in the database.
  - Access to data by the offender is controlled through the use of the PIN and the hand biometric scan. 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 reports through the kiosk self-service technology. If

there is no by-pass, the PIN and hand biometric scan are required every time the offender reports through the kiosk self-service technology.

- Access to the data by CSOSA staff members is controlled by username and password. Each time a CSOSA staff member logs onto the kiosk system, his/her username and password are verified by Active Directory as being a successful match before access to the kiosk system is given.
- All staff access within the kiosk system is controlled by role. Roles define who can do what within the kiosk system. Please see the response to Question 6.1 for a description of the roles in the kiosk system.

- Administrative controls:
  - The kiosk 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 kiosk system constitutes agreement to be monitored through a warning that displays when he/she logs into the kiosk system.
  - CSOSA Office of Information Technology and CSOSA Office of General Counsel are working on an "offender" warning that will display when the offender logs into the kiosk self-service technology as an on-going reminder of the consent to provide the information, of CSOSA's uses of the information, and consent to being monitored.
  - System logs are a critical component of managing authorized and unauthorized access to the kiosk system. The IIS logs monitor accessing of the kiosk application, the SQL Server logs monitor accessing of the kiosk 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 kiosk 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 kiosk servers (kiosk application server, kiosk 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 kiosk system (e.g. review of the Kiosk 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 kiosk system are still in progress (not completed). Completion of the following activities is critical to establishing and maintaining security for the kiosk system, including privacy information:

- Privacy Impact Assessment review and the System of Record determination.
- If the kiosk 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 Kiosk 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.

Providing the offender with additional opportunities to consent to uses is currently in progress. At the time that CSOSA implements the revised version of the kiosk system CSOSA will:

- Provide an enhanced orientation to the kiosk 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.
- Enhance the Kiosk 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.

Offenders who agree to enroll in the kiosk program sign a Kiosk Incentive Behavior Contract. This is at the time of orientation. The offender's signature on the contract implies the offender agrees to all aspects of the kiosk program, including consent to provide the information and understanding of how CSOSA uses the information. Consent would be assumed to cover all uses documented in the orientation materials and Kiosk Enrollment Receipt.

On-going consent to providing the information is assumed each time the offender reports through the kiosk self-service technology. CSOSA Office of Information Technology is working with CSOSA Office of General Counsel to design an "offender" specific warning banner to display when the offender is reporting through the kiosk self-service technology as an on-going reminder of the consent to provide the information and of CSOSA's uses of the information.

Through the kiosk, the offender maintains his/her:

- home address, home phone and cell phone information
- employment information
- school and/or training information
- emergency contact information
- must report if he/she has been rearrested

The offender is expected to maintain complete and accurate information listed above. The offender does not have the option to decline to provide some of the information. If an offender does choose not to provide any, some, or all of the information during monthly reporting, the offender will be "un-enrolled" from the kiosk program and access to the kiosk self-service

technology will be disabled. The offender will continue reporting in-person to his/her assigned Community Supervision Officer until the end of his/her period of supervision.

Use of the kiosk self-service technology by approved enrolled offenders is considered a privilege, and not a requirement or a right of supervision. An offender who is approved for kiosk reporting can opt out of using the kiosk system. If the offender does opt out, he/she will continue reporting in-person to his/her assigned Community Supervision Officer until the end of his/her period of supervision.

7.2 What procedures will allow individuals to access their information?

In addition to the offender's use of the kiosk self-service technology to access his/her 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?

Yes. Offenders who are enrolled in the kiosk program can access, review, update and change their residence, employment, school and emergency contact information through the kiosk self-service technology.

If the offender has concerns about information in the kiosk system that he/she cannot maintain, 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.

7.4 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 kiosk system, CSOSA Office of Information Technology will work with CSOSA Community Supervision Services and CSOSA Office of General Counsel to review the materials used at orientation, and confirm and/or enhance the materials 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. In reviewing and revising the orientation materials with the CSOSA staff members responsible for the orientation, those staff members will be given "re-fresher" training on privacy. Preparing to give and presenting the orientation will continue to provide mini "re-fresher" training sessions as CSOSA staff members will be required to explain the privacy implications to the offenders who are being enrolled in the kiosk program.

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. In addition, CSOSA staff members responsible for offender orientation to the kiosk self-service technology will be reminded of the privacy aspects of the kiosk system and kiosk self-service technology while conducting each orientation.

The Community Supervision Officers responsible for the offenders reporting through the kiosk self-service technology 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 kiosk 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 Kiosk System Security Plan:
  - Documents the boundaries of the kiosk 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 kiosk system in order to align use of the kiosk 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 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 kiosk system, and that the information in the kiosk 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 kiosk 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 kiosk system: The review of offender interaction with the kiosk system is a key source for validating that the information in the kiosk system is used for the stated practices. This includes review of successful reporting sessions, percentage compliance with the reporting frequency and window by offender and across all offenders, CSOSA staff member frequency of successful validations of information entered by the offender (e.g., offender resides or works where he/she says based on a physical visit to the location or phone call with the employer), number of requests by offenders for assistance with the kiosk self-service technology, and offender feedback about issues and problems with the kiosk self-service technology.
- Review of staff actions and use of reports: The review of CSOSA staff member interaction with the kiosk system is another key source of validation that the information in the kiosk system is used for the stated practices. This includes the frequency which

CSOSA staff members have to maintain offender information in the system, the number of successful housing and employment verifications completed based on information entered by the offender into the kiosk self-service technology, the number of in-person interactions with the offenders, and the number of offenders that are disabled from reporting through the kiosk self-service technology – for completion of the period of supervision, and for non-compliant behavior. 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 kiosk 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 kiosk system are still in progress (not completed). Completion of the following activities is critical to establishing and maintaining accountability for the kiosk system, including privacy information:

- Privacy Impact Assessment review and the System of Record determination.
- If the kiosk 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 Kiosk 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.