Court Services and Offender Supervision Agency (CSOSA)

Personnel Security Information System (PSIS) Privacy Impact Assessment

CONTROLLED UNCLASSIFIED INFORMATION

_____, 2020

Office of Security
Court Services and Offender Supervision Agency
800 North Capitol Street, NW, Washington, DC 20002

Overview of Personnel Security Information System (PSIS)

The Court Services and Offender Supervision Agency (CSOSA) core mission is to effectively supervise adults under our jurisdiction, to enhance public safety, reduce recidivism, support the fair administration of justice, and promote accountability, inclusion and success through the implementation of evidence-based practices in close collaboration with our criminal justice partners and the community. To further this mission, the Office of Information & Technology (OIT) and the Office of Security (OS) established the Personnel Security Information System (PSIS) to assist authorized CSOSA staff with effectively and efficiently tracking and managing the background investigation and clearance process for prospective employees, contractors, and current employees and contractors employed by CSOSA.

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

1. Description of the System

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

The Personnel Security Information System (PSIS) electronic tracking database system enables staff to readily identify the information currently gathered on an individual, and at what stage in the investigation process an individual's particular background investigation/re-investigation and clearance is in. Staff members from CSOSA's Office of Security (OS) and the Office of Information Technology (OIT) created and custom designed the PSIS computer system to assist authorized CSOSA OS staff members with effectively and efficiently tracking and managing the background investigation and clearance process for prospective employees, contractors and the 1000+ employees and contractors employed by CSOSA.

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

CSOSA, as a Federal agency employer, is tasked with ensuring that the personnel that work at or perform work for the agency have passed a background check and security clearance before they are hired to handle data and information collected, modified, used, analyzed and stored by the agency as part of its business operations. In order to accomplish this task, the agency collects information, including PII, on each individual who seeks employment, to determine an individual's suitability for employment by the Federal government as an employee or as a contractor in a sensitive or public trust position. Through the employment application and other

personnel forms, the agency collects from the individual information regarding his/her current and prior addresses, telephone numbers, current and prior employment, school, collateral contacts (others who know the individual well) and military service. The agency uses PII information from these forms in the background investigation and clearance process. Some of the information from these forms is entered into PSIS to help track the investigation/clearance through the background check and the security clearance process.

The agency is also required to conduct background and security checks to confirm/re-establish the ongoing employment eligibility for current employees and contractors who work for CSOSA.

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

PSIS is currently in operation. PSIS began operation in August 2015.

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

This is a new PIA.

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

The system is operated by the agency.

2. Legal Authorities and Other Requirements

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

Executive Authority for collecting this information includes:

- Office of Management and Budget ("OMB") Optional Form 306 – Declaration for Federal Employment: Section 1302, 3301, 3304, 3328 and 8716 of title 5, U.S. Code. Section 1104 of title 5 allows OPM to delegate personnel management functions to other Federal agencies.

CSOSA Policy Statement 5800 provides guidance on responsibilities, procedures, and adjudication guidelines for background investigations including preliminary appointment requirements, preliminary background checks, background investigations, and adjudication.

2.2. System of Records Notice (SORN) Requirement: Is the information in this system retrieved by a name or a personal identifier? If so, this system will need to be covered by a Privacy Act SORN.

Yes, for authorized users of PSIS, the system will support a search on prospective employees and contractors and all active employees including interns, student trainees, temporary hires and contractors/consultants by name or personal identifier.

2.3. Records Management Requirement: Does a records retention schedule, approved by National Archives and Records Administration (NARA), exist for the records contained in this system? If yes, please provide the NARA schedule number.

Yes, the records retention schedule for PSIS is (DAA-GRS2017-0006-0025) has been submitted by CSOSA to NARA for review and approval.

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

There is no automated process for removing data from PSIS. Records in PSIS that are marked "in destruction" remain in PSIS until a request is received from the users to logically/physically delete those records (deletion must be completed by someone with database access).

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

Threats to privacy would be through compromise of the data in the database. OIT uses a number of controls: splitting of roles involved with granting user access, strong passwords, Hypertext Transfer Protocol Secure (https) encryption, Activity Directory authentication, transparent data encryption, encrypted data exchanges, and a separate subnet specifically for systems associated with security, and other procedural and system controls to ensure that from a database standpoint, the information is handled, retained, managed and accounted for appropriately.

3. Characterization and Use of Information

Collection

3.1. Select the specific personal information data elements (e.g. name, email, address, phone number, date of birth, social security number, etc.) that the system collects, uses, disseminates, or maintains.

Identifying Numbers					
Social Security	X	File/Case ID	X	Financial Account	
Taxpayer ID		Driver's License		Financial Transaction	
Employee ID	X	Credit Card			

Other identifying numbers (please specify): PSIS tracks the barcode number associated with the hard copy file. The Employee ID is assigned by PSIS. It does not display through the user interface. It is used by the database to maintain the integrity of the data across the tables in the relational database.

General Personal Data					
Name	X	Date of Birth	X	Religion	
Maiden Name		Place of Birth	X	Financial Information	
Alias		Home Address		Medical Information	
Gender		Telephone Number		Military Service	
Age		Email address		Physical Characteristics	
Race/Ethnicity		Education			
Other general personal data (specify): PSIS tracks both the Place of Birth (State if USA or Country), and City of Birth (text field)					

Work-related Data					
Occupation		Telephone number		Salary	
Job title		Email address		Work history	
Work address		Business associates			
Other work-related data (please specify): Work-related data in PSIS includes location of the hard copy file, employee type, Department, company (if a contractor), entrance on duty date, position sensitivity, and separation date. If the person is a contractor, the name of the Contract Specialist and the Contract Number are also tracked.					

Distinguishing Features/Biometrics					
Fingerprints		Photos		DNA profiles	
Palm prints		Scars, marks, tattoos		Retina/iris scans	
Video recording/signatures		Vascular scan		Dental profile	
Other distinguishing features/biometrics (please specify): There is no biometric information or photos in PSIS.					

System admin/audit data					
User ID	X	Date/time of access	X	ID files accessed	X
IP address	X	Queries run	X	Contents of files	X
Other system admin/audit data (please specify): System admin/audit data is collected on users of PSIS. The purpose of collecting this information is for troubleshooting problems (e.g., enables OIT to view error logs to see where a particular transaction is failing. PSIS does have a significant reporting capability (queries run) – access to and running of reports is logged. At the request of the users, the database has SQL triggers to capture specific details about data changes: previous value, new value, and who made the change. Log files are maintained at the database, application, system and network levels.					

3.2. Indicate the sources of the information in the system (e.g., individual, another

agency, commercial sources, etc.) and how the information is collected from stated sources (paper form, webpage, database, etc.).

The information is collected from the individual that is seeking employment with CSOSA. This information is received in person, by telephone, email or fax. Also other investigative agencies provide investigation data. This information is put into PSIS.

Directly from individual about whom the information pertains					
In person	X	Hard copy: mail/fax	X	Online	X
Telephone	X	Email	X		
Other (please specify):					

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

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

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

Data is entered, retrieved, viewed, and updated through the application user interface by authorized staff members in the Office of Security. Once saved, the data is stored in the PSIS database (separate server, database engine is SQL Server). No data is "stored" (meaning saved) in the application (user interface).

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

Most of the data collected and maintained in the PSIS system is to manage the preliminary process, investigation and re-investigation processes. A large part of the information is dates – tracking when certain events happened such as a request for additional information, investigation scheduled date, when fingerprints were checked, approval date, disapproval date, and other similar dates. The results of

those events (such as the results of a drug test, the fingerprints, the actual information provided, the results of credit checks, etc.) are not entered into PSIS. The system does have an "Activities" section which allows staff members to enter notes pertaining to the actions taken regarding the file (e.g., such as a transfer of the hard copy file to the file room). There is limited employee information in PSIS.

Threats to privacy based on the information collected and the sources of information include a compromise of the database. We use a number of controls: splitting of roles involved with granting user access, strong passwords, https, Activity Directory authentication, transparent data encryption, IP specific firewall rules, and a separate subnet to ensure that from a database standpoint, the threats to data compromise or loss are minimized.

Purpose and Use of the System

3.5. Describe how and why the system uses the information to achieve the purpose stated in Question 1.2 above.

Office of Security staff members use the information in PSIS to track and manage the investigation and re-investigation (every 5 years) processes. Since some actions in the clearance processes are completed by the person proposed for investigation, or other agencies, it is important for the Office of Security to track all steps in the process, including when requests are made, when information is received, when items are scheduled, and when completed in order to ensure completion of the process and to accurately report the status at an individual case level, and at aggregate levels (such as number of cases adjudicated in a year). The reports available in PSIS provide data used in the management of cases, such as additional information that is overdue to be submitted, missed scheduled drug tests, new cases and assignments, where the hard copy file is located, and similar type inquiries and actions. In addition, the information collected from the security forms are used to conduct agency preliminary security checks (such as, criminal history checks, credit checks and other agency checks).

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

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

Social Security Numbers

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

The agency collects the individual's Social Security Number (SSN) to help distinguish between individuals who may have the same name and date of birth. The SSNs are used to conduct credit checks. Each individual completes a credit release. The SSN is also used to conduct the criminal background checks. The SSN is entered into PSIS. The OMB Optional Form 306 and the Standard Form 85P where this information is obtained and collected include the Privacy Act and Public Burden Statements, and explain to the individual who completes the forms that providing PII on the forms is voluntary. However, if a person declines to provide the information it could have a negative impact on the individual's background and security clearance approval. The SSN is also used to confirm/verify the identity of the individual and to confirm that the correct record in PSIS is being changed or updated.

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

There were no alternatives considered in the collection of SSN. The alternative that was implemented is that SSN is not used as the key in the relational database in PSIS. The key/foreign key in the relational database is Employee ID, which is assigned by PSIS and used by the system to maintain data integrity across the tables within the database. The Employee ID is not visible through the user interface.

4. Notice

4.1. How does the system provide individuals notice about the collection of PII prior to the collection of information (i.e. written Privacy Act notice, link to a privacy policy, etc.)? If notice is not provided, explain why not.

The agency provides notice to individuals who seek employment with the Federal government as an employee or contractor when they complete and sign certain application and personnel forms. Through the instructions in the application and personnel forms, the agency provides written notice to the person that upon their signature on the forms, the agency may use certain personal information to conduct a background check and security clearance. The personnel forms that the agency uses to collect PII, of which some of the information is entered into the PSIS database system, for a background check and security clearance are:

- OMB Optional Form 306 – Declaration for Federal Employment.
- Standard Form 85P – Questionnaire for Public Trust Positions.
- CSOSA-SEC-0010 – Security Form for Temporary Contractors or Employees.
- CSOSA-SEC-0008 – Release for consumer/credit reports.

The individuals receive notice when they complete and sign the background investigation forms. These forms hereinafter will be collectively referred to as "the Forms". Information about the Privacy Act and Public Burden Statements are included in the instructions for the OMB Optional Form 306 and the Standard Form 85P. The PII collected from the Forms that will be entered into the PSIS database consists of an individual's:

- Last Name
- First Name
- Middle Name
- Suffix
- Social Security Number
- Date of Birth
- Place of Birth
- City of Birth

Although the agency does not provide specific notice to individuals that their PII will be entered into the PSIS database system, the agency provides notice that the agency's collection of their PII will be necessary to complete the background investigation and clearance process. Authorized agency personnel will enter the PII data listed above into PSIS to help facilitate and track any information related to the background investigation and clearance process. Individuals will receive notice through the SORN published with the Federal Register that the agency has developed the PSIS database system to input specific PII and use this information to track the background and security clearance for the individual as it moves through the clearance process.

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

The personnel forms that the agency uses to collect PII, of which some of the information is entered into the PSIS database system, for a background check and security clearance are:

OMB Optional Form 306 – Declaration for Federal Employment
This form has a Privacy Act Statement listed on top of the form, prior to data collection.

Standard Form 85P – Questionnaire for Public Trust Positions
This form provide disclosure, Privacy Act routine uses, authority to request and collection information, as well as an authorization for release of information.

CSOSA-SEC-0010 – Security Form for Temporary Contractors or Employees
This form provides notice on the top of the page that it the form will be used by the Office of Security to conduct a CSOSA background check. Please visit the link here: https://intranet.csosa.gov/Forms/SEC0010-Temp-Contractor-Form-10182013.pdf

CSOSA-SEC-0008 – Release for consumer/credit reports
This form provides notice within the document, notifying applicants that the form is a release for CSOSA to obtain one or more consumer/credit reports about. Please visit the link here: https://intranet.csosa.gov/Forms/SEC_0008_Credit_Release_Form.pdf

The Privacy Act Statement is provided below:

Authority:
Information maintained in the system is collected pursuant to 5 C.F.R. § 731.103, 5 C.F.R. § 731.401 - § 731.404, CSOSA Policy Statement 5800, and Security Requirements for Government Employees; and E.O. 9397* (SSN), as amended.

Purpose:
The agency collects PII from each individual who seeks employment, to determine an individual's suitability for employment by the Federal government as an employee or as a contractor in a sensitive or public trust position.

Routine Use:

Standard CSOSA Routine Uses:

- *For Law Enforcement Purposes*: To disclose pertinent information to the appropriate Federal, state, or local agency responsible for investigating, prosecuting, enforcing, or implementing a statute, rule, regulation or order, where CSOSA becomes aware of an indication of a violation or potential violation of a civil or criminal law or regulation.
    - *For Litigation*: To disclose information to the Department of Justice for the purpose of representing CSOSA, or its components or employees, pending or potential litigation to which the record is pertinent.
    - *For Judicial/Administrative Proceedings*: To disclose information to another Federal agency, a court, grand jury, or a party in litigation before a court or administrative proceeding being conducted by a Federal agency, when the Federal Government is a party to the judicial or administrative proceeding.
    - *For National Archives and Records Administration*: To disclose information to the National Archives and Records Administration for use in records management inspections conducted under the authority of 44 U.S.C. §§ 2904 and 2906.

- *For Congressional Inquiry*: To provide information to a Member of Congress or staff acting upon the Member's behalf when the Member or staff requests the information on behalf of, and at the request of, the individual who is the subject of the record.

- *For Data Breach and Mitigation Response*:

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

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

Disclosures:

Disclosure of PII is voluntary; however, failure to provide the information may result in our inability to grant your access to our facilities.

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

At the time the individual completes the Forms for employment as an employee, volunteer, intern, or contractor, the person will have the opportunity to decline to provide PII. The requirements of the Privacy Act and Public Burden Statements are included in the instructions for the OMB Optional Form 306 and the Standard Form

85P. The Forms also include information that disclosure of PII is voluntary and that the agency will collect and use their Social Security Number and other information to conduct a background investigation for a security clearance. The Forms inform the individual that withholding the information could negatively impact the individual's security clearance.

Once the Forms have been completed, signed, and submitted to the agency, authorized CSOSA Office of Security staff members start the background investigation and clearance process. The individual may withdraw his or her application at any time, however, it is unlikely the individual will receive a security clearance to work at CSOSA if the application is withdrawn.

During the agency's re-investigation of an employee's or contractor's background, the individual will have the opportunity to review and "re-consent" to the use of their PII information for a background investigation. The individual will complete and sign a new OMB Optional Form 306 and the Standard Form 85P.

If an employee or contractor determines that the agency has inaccurate, incomplete, out of date, or irrelevant information, the individual will have an opportunity to submit new information so that the information can be updated in PSIS by authorized CSOSA Office of Security staff members.

5. Information Sharing

Internal

5.1. How do agency personnel gain access to the system and the PII (e.g., users, managers, system administrators, developers, contractors, etc.)?

Access to PSIS is tightly controlled. The CSOSA Director of Security authorizes PSIS users through the CSOSA Information System Users Access Request Form. The form must be signed by the Director of Security, or the Deputy Director of Security or the Security Specialist responsible for PSIS in the absence of the Director of Security. If the form is not signed by one of these individuals, access to the PSIS will not be allowed.

Access to PSIS by CSOSA Office of Security staff members is controlled by username and password. CSOSA uses Microsoft Active Directory, a directory used by OIT to maintain a central username and password for each CSOSA staff member. Each time an authorized CSOSA staff member logs into PSIS, his/her username and password is verified by Active Directory before the staff member obtains access to PSIS. A user's role in PSIS (staff member or supervisor) is maintained in the PSIS database and controls the functionality available to the staff member. Authorized users of PSIS have access to the information entered into PSIS on any individual at the individual record level. Report data for staff members is generally limited to cases to which the staff member is assigned. The supervisor functionality in PSIS allows the authorized user

to update dropdown table values; delete pre-appointment, investigation and activity records (e.g., entered in error by a staff member); see report data for a specific staff member or all staff members; and view audit information through the user interface for PSIS.

The CSOSA Director of Security has requested that only one person in the CSOSA OIT provide system and system administrator support to the production PSIS environment since the information is considered highly sensitive. If the Director of Security is unavailable, he/she will designate the responsibilities to the Lead Personnel Security Specialist. A CSOSA Information Systems Privileged Access Request Form, signed by the CSOSA Director of Security, authorizes that individual to provide system and system administrator support, including adding/updating/deleting user roles in the PSIS database. This limits the potential for multiple points of compromise of the data in PSIS as only one person from OIT has access to PSIS to provide system administrator support. If that individual should become unavailable, a new CSOSA Information Systems Privileged Access Request Form for another Developer would need to be prepared, signed and processed to give the new Developer the appropriate access to PSIS application and data.

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

Access to PSIS is limited to Office of Security (OS) staff members. If an internal CSOSA staff person not in the Office of Security needs information from PSIS (such as the status of a background investigation of a new hire), that information will be provided by the Office of Security at the discretion of the OS Personnel Security Specialist. Information is not shared with the Agency's executive leadership.

5.3. What information will be shared and with whom?

First Name, Last Name, and Component is the information that will be shared within the staff via report. This information is shared only within the Office of Security.

5.4. How will the information be shared?

The information is only shared within the OS and is not shared with other CSOSA divisions or outside offices. The information may be forwarded to other OS staff members, in the form of a report, to allow for correction of errors on cases they have processed or to start the investigation or reinvestigation process.

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

The information in PSIS is shared with staff in the OS for the purposes of ensuring data accuracy on cases that they have processed or to initiate the investigation or

reinvestigation process. PSIS information is not shared with any other CSOSA Offices.

5.6. Describe controls that the program offices and/or components have put into place in order to prevent or mitigate threats to privacy in connection with the disclosure of information.

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

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

All computer systems at CSOSA, including PSIS, are monitored through computer security software programs. All CSOSA staff members (employees, contractors, anyone with access to CSOSA computer systems and/or the CSOSA network) are notified that computer use is subject to monitoring and use of the network and systems is consent to that monitoring. There is a warning on the log in screen for PSIS that tells authorized users that use of the system may be monitored, intercepted, recorded, read, copied or captured. See the responses to Questions 4.1 and 4.2.

The PSIS database includes fields that identify who created the record/change, the date it was created, by whom it was updated, and the date the information was updated when a record in that table is created/updated/ revised/deleted. In addition, a separate auditing feature was added to PSIS to track any changes that are made to the different fields in the records in the database. The auditing feature shows the value for the field before the change, the value of the field after the change, who made the change and when the change was completed. Authorized users in the supervisor role have access to the audit information for any individual's record in PSIS through the user interface, and can review the audit data when required if there are concerns about an individual's information in PSIS, or if unauthorized access is suspected. The approved OIT staff member will review the record change information, when required, if there are concerns about an individual's information in PSIS, or if unauthorized access is suspected, and periodically, to confirm that the data is protected and no unauthorized access has occurred.

External

5.8. Will the information contained in the system be shared with external entities (e.g. another federal agency, District of Columbia agency, etc.)?

The information that entered into PSIS about an individual's background investigation or clearance check will not be shared or made available to CSOSA employees, other agencies or external third parties, except as permitted under the Privacy Act of 1974.

Information about an individual that needs to be provided to another agency, external third party or organization involved with the background investigation and security clearance process will be only shared by providing the paper forms signed release by the individual, or entered directly into secured systems owned/operated by that agency, external third party or organization (e.g., the use of Equifax to run a credit check). The Office of Security (OS) staff are responsible for assuring proper use of the data. Only OS staff enter information in PSIS, any system owned/operated by another agency, third party or organization. There is no system to system exchange of information.

5.9. What information will be shared and with whom?

If information in PSIS needs to be shared with a third party or organization involved with the investigation, background investigation information such as dates and the type of investigation is shared with external third party or organizations. Information is only shared by providing the signed release from the individual. This information is given via memorandum form and not through the PSIS system. There is no system-to-system exchange of information.

5.10. What is the purpose of sharing the specified information with the specified external entity? Does this purpose align with the stated purpose in Question 1.2 above?

PII is shared with external entity for additional record checks, such as credit check, which is part of the overall background and security check process.

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

The background information retrieved from PSIS and provided to the external entity in the form of a letter by a member of the Security Staff. The information is used by the external entity to ensure the individuals have the appropriate background investigation for the position they will be occupying or the work they will be conducting.

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

The data is protected by password. Each Security Staff member has a unique user name and password to log into the PSIS database. The CSOSA Director of Security has requested that only one person in the CSOSA Office of Information Technology provide system and system administrator support to the production PSIS environment since the information is considered highly sensitive. If the Director of Security is unavailable, he/she will designate the responsibilities to the Lead Personnel Security Specialist. A CSOSA Information Systems Privileged Access Request Form, signed by the CSOSA Director of Security, authorizes that individual to provide system and system administrator support, including adding/updating/deleting user roles in the PSIS database. This limits the potential for multiple points of compromise of the data in PSIS as only one person from the

Office of Technology has access to PSIS to provide system administrator support. If that individual should become unavailable, a new CSOSA Information Systems Privileged Access Request Form for another Developer would need to be prepared, signed and processed to give the new Developer the appropriate access to PSIS application and data.

5.13. Is the external information sharing pursuant to a Computer Matching Agreement (CMA), Memorandum of Understanding (MOU), or other type of approved sharing agreement with another agency?

There is no data sharing from or to PSIS.

6. Consent and Redress

6.1. How will individuals be notified if there are any changes regarding how their information is being collected, maintained, or disseminated by the system?

The Director of the Office of Security will notify individuals by email if any changes should occur on how their information is being managed within the PSIS database.

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

There are no procedures that allow an individual to directly access his/her information in PSIS. Access to PSIS is limited to CSOSA Office of Security staff members. Individuals seeking access to their information entered into PSIS must submit a Freedom of Information Act (FOIA) request to the Office of Personnel Management (OPM). OPM is the owner of the background investigation information. OPM processes the FOIA requests.

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

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

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

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

In addition, the requestor should provide the following:

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

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

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

There are no written procedures in place to correct the inaccurate information. However, if during the preliminary or background investigation security process any information that has been entered in PSIS needs to be changed, CSOSA Office of Security staff members will update the information in PSIS. If during the adjudication process information that has been entered in PSIS on an individual changes, authorized CSOSA Office of Security staff members will update PSIS. If any information in PSIS is inaccurate, incomplete, out of date, or irrelevant, an authorized CSOSA Office Security Staff member can generate reports within the system to find errors and update the information. This database is used for tracking purposes within CSOSA Office of Security and the information entered will not impact subject individual's suitability.

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

Due to the sensitive nature and purpose of PSIS, the Office of Security Staff members are responsible for entering the information. If any information has to be corrected, the Office of Security will contact the individual obtain the

information and make the correction.

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

During the preliminary process, the individuals will have an opportunity to consent or dissent once they submit their security forms (SF-85P or OF-306) to the Office of Security.

6.6. How will the agency provide notice to individuals that their PII information may be shared with other agencies or entities (both internal and external)?

The security forms that individuals are required to complete include a notice that PII may be shared with other agencies or entities.

7. Information Security and Safeguards

7.1. Does the component office work with their Chief Information Officer (CIO) to build privacy and security into the system and build privacy extension to the extent feasible?

Yes.

7.2. Do contractors have access to the system?

Yes. The Office of Security can hire a contractor who will have access to the system to perform the necessary job related functions. The individual will be required to complete the necessary form for access. The Director of Security has the authority to approve the request.

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

Access to PSIS is tightly controlled. The CSOSA Director of Security authorizes PSIS users through the CSOSA Information System Users Access Request Form. The form must be signed by the Director of Security, or the Deputy Director of Security or the Security Specialist responsible for PSIS in the absence of the Director of Security. If the form is not signed by one of these individuals, access to the PSIS will not be allowed.

The form is then reviewed by an account administrator at CSOSA. If approved, a ticket for OIT Customer Support is created for the Active Directory account. Once the Active Directory account is established, the developer approved and responsible for PSIS creates the user/user role in PSIS.

The CSOSA Director of Security has requested that only one person in the CSOSA

OIT provide system and system administrator support to the production PSIS environment since the information is considered highly sensitive. If the Director of Security is unavailable, he/she will designate the responsibilities to the Lead Personnel Security Specialist. A CSOSA Information Systems Privileged Access Request Form, signed by the CSOSA Director of Security, authorizes that individual to provide system and system administrator support, including adding/updating/deleting user roles in the PSIS database.

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

Physical controls:

- Limiting access to CSOSA Office of Security office spaces by key access control 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.
- Utilizing cipher locks to control access to CSOSA Office of Security staff member offices.
- Ensuring workstations by authorized CSOSA Office of Security staff members are located within their office spaces.
- Prohibiting staff from connecting personal laptops, thumb drives, or other electronic devices to CSOSA's network.
- When working remotely, using user authentication in the form of an assigned PIN from agency phones, in addition to the username and password, to authenticate access to the network.
- The servers running the PSIS application and housing the PSIS database are located in CSOSA's data center. Access to CSOSA's data center is restricted and limited to 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 PSIS run on the CSOSA network and are located behind the network internal firewall.
- The PSIS application is a web-based program and available on CSOSA's Intranet. All workstation access to the PSIS application server is protected by a Secure Socket Layer (SSL) Certificate, which encrypts information between the workstation and PSIS server.
- The physical database is protected using transparent data encryption, which protects the data when in the database.
- Access to the data by CSOSA staff members is controlled by username and password. Each time an authorized CSOSA Office of Security staff member logs onto PSIS, his/her username and password are verified by Active Directory as being a successful match before access to PSIS is given.
- The servers that support the PSIS application and database have been moved to an

isolated network segment.

Administrative controls:

- The PSIS 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.
- The PSIS's audit feature captures audit trail information at the field level in the database. A separate auditing feature was added to PSIS to track all changes made to certain fields in the database – the value before the change, the value after the change, who made the change and when the change was completed. All fields that are considered PII have this audit feature.
- The PSIS system notifies users when they log into PSIS that users may be monitored when accessing PSIS and any access is consent to being monitored.
- All components on the PSIS server 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 CSOSA Office of Security, CSOSA Office of Information Technology staff members, or an auditor.

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

The current Authority to Operate expires on 5/29/2023.

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

OIT can provide information on who entered data, who changed data, and when.

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

There are no data limitations for PSIS within the Security Office. Every authorized user of PSIS can add/view/update/change any record in PSIS. No one outside of the Security Office has access to the system.

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

The logs (IIS, SQL Server, server, network) provide the data needed to verify that authorized users are accessing the system, and to search for and identify any unauthorized accesses to the system. The logs are reviewed manually on a periodic basis.

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

Privacy training is covered in the agency's annual IT Security Awareness training which is required for all CSOSA staff members, including CSOSA Office of Security staff members. CSOSA staff members are required to take federally mandated ethics training on an annual basis – which covers appropriate and inappropriate actions and disclosures of information.

Specific to PSIS, CSOSA Office of Security staff members are trained on the PII that is maintained within PSIS, proper retention and disposition of any printed materials, forms or reports, and protecting PII displayed on a workstation or screen from being viewed by personnel or offenders who are not authorized to access PSIS. CSOSA Office of Security staff members are also trained on the handling, review, distribution, filing and disposition of any forms or other hard copy materials associated with the background investigation and clearance process.

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

All authorized users of PSIS, and authorized staff in the Office of Information Technology are responsible for assuring the correct use of the information and safeguarding of PII. The Development Team is responsible for configuring and coding any safeguards into the application. The Infrastructure Team and Development Team are jointly responsible for any safeguards at the server, network, operating system and software levels such as server hardening, patching, configuring security benchmarks, and other similar safeguards.

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

PSIS contains background investigation dates along with names, social security numbers and date of birth. If this information is unlawfully disclosed, there is the possibility that the owner's information can exposed resulting in fraudulent activity.

7.12. If contractors have access to the system, has the agency provided the contractor, who works on the system, a confidentiality agreement or a Non-Disclosure Agreement (NDA)?

No NDA is required. Contractors will complete the necessary security forms and undergo a background investigation by the Office of Personnel Management. A confidentiality agreement is not required. Contractors who have access to the system are confined to same standards and requirements as federal employees.

8. Auditing and Accountability

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

System owners ensure that information is used in accordance with the PIA by ensuring that everyone who has access to the system is well informed of the system's purpose

and understands how to safely handle the PII in the system, by way of training and annual security and privacy assessments.

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

PSIS has several tools and processes associated with the system to mitigate risks, including the processes and tools mentioned in the responses to Questions 3.4, 4.1, 5.6, 7.4, 7.8 and 7.9.

9. Data Quality and Integrity

9.1. How will the information that the agency collects be verified for accuracy and completeness when it is entered into the system?

The prospective employee provides the information on security forms and release forms. When the information is received by the Office of Security a staff member will review it for accuracy and completeness before adding it into the system.

For authorized users of PSIS, the information entered into the system is verified against the change request document – either the Computer Access Form, or the OIT Customer Support portal ticket request.

9.2. Are there any privacy risks for individuals whose information is collected or used by the project that relate to data quality and integrity? If so, how will CSOSA mitigate these risks?

No other known privacy risks other than what is already documented in the responses to Questions 2.5, 3.4 and 8.2.

10. Privacy Policy and Statement

10.1. Has the agency provided a privacy statement or policy for this system and is it provided to all individuals whose PII is collected, maintained or stored?

Yes, the privacy act statement will be provided on the CSOSA forms SEC 0010 and 0008.

The personnel forms that the agency uses to collect PII for a background check and security clearance are:

- OMB Optional Form 306 – Declaration for Federal Employment.
- Standard Form 85P – Questionnaire for Public Trust Positions.
- CSOSA-SEC-0010 – Security Form for Temporary Contractors or Employees.
- CSOSA-SEC-0008 – Release for consumer/credit reports.

Some of the information is entered into the PSIS. Information about the Privacy Act and

Public Burden Statements are included in the instructions for the OMB Optional Form 306 and the Standard Form 85P. Policy Statement 5800 (PS 5800) provides authority for the collection of information obtained from the CSOSA-SEC-0010 and CSOSA-SEC-0008 forms.

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

CSOSA's privacy policy is publicly viewable on the agency's public website at:

https://www.csosa.gov/privacy-policy

Authorizing Signatures

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

___Andrew Thomas_____
System Owner Name (Please Print)

9/23/2020

X Andrew Thomas

Andrew Thomas
Director of Security
Signed by: ANDREW THOMAS

_____Johnathan Raford_____
Privacy Program Manager Name (Please Print)

X JOHNATHAN RAFORD Digitally signed by JOHNATHAN RAFORD Date: 2020.09.24 12:09:07 -04'00'

Johnathan Raford

_____Sheila Stokes_____
Senior Agency Official for Privacy (Print)

X SHEILA STOKES Digitally signed by SHEILA STOKES Date: 2021.04.15 10:44:27 -04'00'

Sheila Stokes