Court Services and Offender Supervision Agency
Pretrial Services Agency
for the District of Columbia
Office of the General Counsel
Office of Legal Services

POLICY STATEMENT

Privacy
Number: 1113
Effective Date: 4/15/2021
Review Due Date:4/15/2023

RICHARD TISCHNER
Digitally signed by RICHARD TISCHNER
Date: 2021.04.09 15:02:47 -04'00'

Richard Tischner
Director, CSOSA

Digitally signed by Leslie C. Cooper
Date: 2021.04.09 11:54:23 -04'00'

Leslie Cooper
Director, PSA

Table of Contents

Overview 2
Policy 5
Definitions 9
Roles and Responsibilities 14

Overview

Background

The Privacy Act of 1974, as amended, 5 U.S.C. § 552a, balances the government's need to maintain information about individuals with the rights of individuals to be protected against unwarranted invasions of their privacy. The Privacy Act provides protections to individuals in four (4) primary ways:

- Restricts disclosure of personally identifiable information (PII) maintained by agencies;
- Grants individuals increased right of access to agency records maintained on them;
- Grants individuals the right to seek amendment of agency records maintained on them upon a showing that the records are not accurate, relevant, timely, or complete; and
- Establishes a code of "fair information practice principles" that requires agencies to comply with statutory norms for collection, maintenance, use, and dissemination of information about individuals that is maintained in systems of records by federal agencies.

This Policy Statement affirms Court Services and Offender Supervision Agency's (CSOSA or Agency) and Pretrial Services Agency for the District of Columbia's (PSA or Agency) (or collectively, the Agencies) commitment to abide by the requirements of the Privacy Act and all applicable laws and regulations. It uses the "fair information practice principles" as the basis for the Agencies' strategic, risk-based privacy policy.

Summary of Changes

- Separation of FOIA policy information from the Policy Statement.
- Separation of policy from procedures.
- Definition of additional terms.
- Clarification of roles and responsibilities.

Coverage

This Policy Statement applies to all CSOSA and PSA employees, contractors, and interns who collect, maintain, use, and disseminate personally identifiable information in the performance of official duties.

Continued on next page

Overview, Continued

Authorities

- Privacy Act of 1974, 5 U.S.C. § 552a.
- Freedom of Information Act (FOIA), 5 U.S.C. § 552.
- E-Government Act of 2002, Pub. L. 107-347, codified at 44 U.S.C. § 3601.
- Federal Information Security Modernization Act (FISMA) of 2014, 44 U.S.C. Chapter 35.
- Privacy Procedures for Personnel Records, 5 C.F.R. Part 297.
- Disclosure of records, 28 C.F.R. Part 802.
- National Institute of Science and Technology Special Publication (NIST SP) 800-53, Security and Privacy Controls for Information Systems and Organizations, Revision 5 (September 2020).
- NIST SP 800-122, Guide to Protecting the Confidentiality of Personally Identifiable Information (PII) (April 2010).
- President of the United States Memorandum for the Heads of Executive Departments and Agencies, Transparency and Open Government, 74 Fed. Reg. 4685 (January 21, 2009).
- OMB Circular A-130, Managing Information as a Strategic Resource, 81 Fed. Reg. 49689 (July 28, 2016).
- OMB Memorandum M-03-22, Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002 (September 26, 2003).
- OMB Memorandum M-07-16, Safeguarding Against and Responding to the Breach of Personally Identifiable Information (May 22, 2007).
- OMB Memorandum M-17-12, Preparing for and Responding to a Breach of Personally Identifiable Information (January 3, 2017).
- OMB Memorandum M-21-02, Fiscal Year 2020-2021, Guidance on Federal Information Security and Privacy Management Requirements (November 9, 2020).
- OMB Memorandum M-21-04, Modernizing Access to and Consent for Disclosure of Records Subject to the Privacy Act (November 12, 2020).
- Electronic Communications Privacy Act of 1986, 99 Pub. L. 508, codified at 18 U.S.C. §§ 2510–2522, 2701–2709.
- Health Insurance Portability and Accountability Act of 1996, as amended (HIPAA), Pub. L. 104-191.
- HIPAA, Standards for Privacy of Individually Identifiable Health Information, 45 C.F.R. Parts 160 and 164.
- Confidentiality of Substance Use Disorder Patient Records, 42 C.F.R. Part 2.

Continued on next page

Overview, Continued

Authorities, continued

- DC Mental Health Information Act, D.C. Code Title 7, Chapter 12.
- Federal Records Act, 44 U.S.C. §§ 3101-07, 3301-14.
- Executive Order 13556, Controlled Unclassified Information (November 4, 2010).

Disclaimer

The contents of this guidance do not have the force and effect of law and are not meant to bind the public in any way. This document is intended only to provide clarity to the public regarding existing requirements under the law or agency policies.

References

- NIST SP 800-37, Risk Management Framework for Information Systems and Organizations, revision 2 (December 2018).
- NIST SP 800-161, Supply Chain Risk Management Practices for Federal Information Systems and Organizations *(*April 2015).
- NIST SP 800-171, Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations, revision 2 (February 2020).
- OMB Circular A-108, Federal Agency Responsibilities for Review, Reporting, and Publication under the Privacy Act *(*December 23, 2016).
- OMB Memorandum M-01-05, Guidance on Inter-Agency Sharing of Personal Data-Protecting Personal Privacy (December 20, 2000).
- PS 2036 Information Technology Security, CSOSA (March 20, 2020).
- PS 5500 Information Technology Security, PSA (February 11, 2020).
- PS 1111 Records Management, CSOSA (September 21, 2017).
- PS 1008 Records Management, PSA (September 10, 2018)

Supersedes

This Policy Statement supersedes Office of the General Counsel Directive: *Freedom of Information/Privacy Act,* dated October 2, 2000.

Administrator

CSOSA Office of the General Counsel and PSA Office of Legal Services are responsible for the contents of the Policy Statement.

Policy

Introduction

The Agencies' missions specify the purpose for which PII is collected, used, maintained, and shared. The Privacy Act requires all federal agencies to publish in the Federal Register all of their systems of records and list their routine uses for each system. CSOSA's and PSA's systems of records and routine use disclosures are published in the Federal Register. Under the Privacy Act's routine use exception, the Agencies are permitted to release certain information regarding defendants/offenders without their consent, to meet enumerated objectives (e.g., to civil or criminal law enforcement agencies to accomplish their assigned duties).

Framework

The Fair Information Practice Principles (FIPPS) are a set of principles that are rooted in the tenets of the Privacy Act. The FIPPs are a widely accepted framework that provide a universal platform for identifying, assessing, and mitigating privacy risks. The Agencies adhere to FIPPs when collecting, maintaining, using, storing, transmitting, protecting, and destroying PII in all media forms (e.g., electronic, hard copy, visual, or recorded form). FIPPs form the basis of the Agencies' privacy policy and procedures governing the use of PII. These principles are:

- Purpose Specification
- Accountability and Audit
- Data Quality and Integrity
- Data Minimization and Retention
- Individual Participation and Redress
- Security
- Transparency, and
- Use Limitation.

Purpose Specification

The Agencies:

- Document the legal authority that permits the collection, use, maintenance, and sharing of PII; and
- Describe the purpose(s) for which PII is collected, used, maintained, and shared in the Agencies' privacy notices.

Continued on next page

Policy, Continued

Accountability and Audit	The Agencies: • Provide annual training to all employees, contractors, and interns in the proper handling of PII, even when accessing or gathering PII is not part of their regularly assigned duties; • Hold accountable any individual who discloses PII without prior written consent, regardless of whether such disclosure was intentional. The individual may be subject to disciplinary action, criminal penalties, or both; and • Audit the actual use of PII to promote compliance, and identify and address gaps in privacy protection requirements.
Data Quality and Integrity	The Agencies, to the greatest extent practicable: • Ensure that PII is accurate, relevant, timely, and complete; and • Collect PII directly from the individual.
Data Minimization & Retention	The Agencies: • Identify and only collect PII that is directly relevant and necessary to accomplish the Agencies' mission-related functions and operations; • Reduce the use of specified PII (e.g., social security number [SSN]) and/or use alternatives to SSN as personal identifiers, where feasible; • Retain PII only as long as is necessary to fulfill the Agencies' mission-related functions and operations; and • Dispose of, destroy, erase, and/or anonymize PII consistent with the Agencies' record retention schedule.

Continued on next page

Policy, Continued

Individual Participation & Redress

The Agencies, to the greatest extent practicable:

- Seek individual consent for the collection, use, dissemination, and maintenance of PII; and
- Provide mechanisms for appropriate access, correction, and redress regarding the Agencies' use of PII.

NOTE: The Agencies offer a digital service option with remote identify-proofing and authentication, to ensure that individuals have the ability to digitally request access to or consent to disclosure of their records. The digital service option is in addition to paper-based or in-person options.

Security

The Agencies:

- Protect PII through appropriate security safeguards based on the PII confidentiality impact level;
- Maintain and update an inventory of all programs and information systems that collect, use, maintain, or share PII; and
- Provide an organized and effective response to privacy incidents via a Breach Response Plan that employs processes, assessments, and procedures.

Transparency

The Agencies:

- Provide public notice regarding:
  - The Agencies' activities that impact privacy, including collection, use, sharing, safeguarding, maintenance, and disposal of PII;
  - The authority that permits the collection of PII and the purpose or purposes for which the PII is intended to be used; and
  - The ability of individuals to access and have PII amended or corrected, if necessary;
- Publish System of Record Notices (SORNs) in the Federal Register for systems containing PII and the Agencies' Privacy Policy on their public-facing websites; and
- Conduct Privacy Threshold Assessments (PTAs) and, if indicated, conduct and publish Privacy Impact Assessments (PIAs) to demonstrate the inclusion of privacy considerations in advance of implementing any new technologies that affect PII.

Continued on next page

Policy, Continued

Use Limitation

The Agencies:

- Use PII solely for the purpose(s) specified in the public notice; and
- Release PII to the public or private entities only in the performance of official duties:
  - For a purpose compatible with the purpose for which the PII was collected;
  - Pursuant to a written request by, or with the prior written consent of, the individual to whom the record pertains; or
  - As permitted by one of the twelve (12) statutory exceptions under the Privacy Act and/or any other applicable law or policy setting forth public access to information.

Definitions

Authentication	Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to a system's resources.
Breach	The loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or any similar occurrence when: • A person other than an authorized user accesses or potentially accesses PII; or • An authorized user accesses or potentially accesses PII for other than an authorized purpose.
Computer Matching Agreement	The Computer Matching and Privacy Protection Act of 1988, Pub. L. 100-503, 102 Stat. 2507, amended the Privacy Act to include provisions governing computer matching activities. Pursuant to 5 U.S.C. § 552a(o)(1), "no record which is contained in a system of records may be disclosed to a recipient agency or non-Federal agency for use in a computer matching program except according to a written agreement between the source agency and the recipient agency or non-Federal agency," provided the agreement meets delineated requirements.
Confidentiality	Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.
Controlled Unclassified Information (CUI)	Information the government creates or possesses, or that an entity creates or possesses for or on behalf of the government, that a law, regulation, or government-wide policy requires or permits an agency to handle using safeguarding or dissemination controls.
Credential Service Provider (CSP)	A trusted entity that issues or registers subscriber authenticators and issues electronic credentials to subscribers. A CSP may be an independent third party or issue credentials for its own use.

Continued on next page

Definitions, Continued

Health Insurance Portability and Accountability Act (HIPAA)	The statute pertaining, among other things, to health insurance portability, pursuant to which regulations were published to govern privacy and security. HIPAA modernized the flow of healthcare information, stipulated how PII maintained by the healthcare and healthcare insurance industries should be protected from fraud and theft, and addressed limitations on healthcare insurance coverage – such as portability and the coverage of individuals with pre-existing conditions.
Identity-Proofing	The process by which a CSP collects, validates, and verifies information about a person.
Incident	An occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits, or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies.
Information System	A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.
Information System Owner	An official responsible for the overall procurement, development, integration, modification or operation and maintenance of an information system.
Personally Identifiable Information (PII)	Any information about an individual maintained by an agency, including: • Any information that can be used to distinguish or trace an individual‘s identity, such as name, social security number, date and place of birth, mother‘s maiden name, or biometric records; and • Any other information that is linked or linkable to an individual, such as medical, educational, financial, email, telephone, and employment information.

Continued on next page

Definitions, Continued

Privacy	An individual's interests in preventing the inappropriate collection, use, and release of PII. Privacy interests include privacy of personal behavior, privacy of personal communications, and privacy of personal data.
Privacy Act Request	• A request to an agency to gain access to an individual's record, such as by another federal agency or law enforcement as required by statute. • A request by any individual to gain access to his/her record or to any information pertaining to him/her which is contained in the system.
Privacy Impact Assessment (PIA)	An analysis of how information is handled to: • Ensure compliance to applicable legal, regulatory, and policy requirements regarding privacy; • Determine the risks and effects of collecting, maintaining and disseminating information in identifiable form in an electronic information system; and • Examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks.
Privacy Threshold Analysis (PTA)	A survey of questions that is prepared for all new information technology systems and any other information technology investment that undergoes substantial modifications. The PTA determines if the investment will be collecting any PII data elements and if a full PIA is required.
Record	Any item, collection, or grouping of information about an individual that is maintained by an agency, including, but not limited to, education, personally identifiable information, financial transactions, medical history, and criminal or employment history and that contains the individual's name, or the identifying number, symbol, or other identifying particular assigned to the individual, such as a fingerprint or voice print or a photograph.

Continued on next page

Definitions, Continued

Routine Use

With respect to the disclosure of a record, the use of such record for a purpose which is compatible with the purpose for which it was collected. In other words, disclosures that are appropriate and necessary for the efficient conduct of government business. 5 U.S.C. § 552a(b)(3) (routine use) is one of the twelve (12) statutory exceptions to disclosure without written consent under the Privacy Act.

Sensitive PII

A subset of PII that, if lost, compromised, or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual. Sensitive PII require stricter handling guidelines because of the increased risk to an individual if the data is compromised.

Examples of Sensitive PII include, but are not limited to:

- Social Security numbers (SSN);
- Driver's license or state identification numbers;
- Passport numbers;
- Alien Registration numbers;
- Financial account numbers;
- Biometric identifiers; and
- Other data, when combined, may also constitute Sensitive PII, such as:
  - Citizenship or immigration status;
  - Medical information;
  - Salary;
  - Ethnic or religious affiliation;
  - Personal email address, address, and phone;
  - Account passwords;
  - Date of birth;
  - Criminal history; or
  - Mother's maiden name.

Continued on next page

Definitions, Continued

System of Records	A group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to that individual.
System of Records Notice (SORN)	Notice published in the Federal Register prior to an agency's collection, maintenance, use, or dissemination of information about an individual.

Roles and Responsibilities

Employees, Contractors, and Interns	• Complete all mandatory information security and privacy awareness training. • Comply with policies and procedures on information security and privacy. • Reduce information security and privacy risks associated with their activities by: – Observing all information security and privacy requirements for collecting, maintaining, using, and disseminating information maintained in the Agencies' systems of records; and – Ensuring that the PII used in carrying out official duties is protected according to Privacy Act and information security requirements. • Adhere to the Agencies' privacy incident reporting procedures and **immediately** report any observed or suspected privacy incidents.
Supervisors thru Deputy Assistant Directors and Associate Directors	• Ensure employees under their direct supervision complete all initial and recurring information security and privacy awareness training within the required time frames. • Provide oversight and quality control measures, as applicable, to ensure: – Employees take reasonable precautions to guard against unauthorized disclosure of PII; – Electronic safeguarding measures are adequate for the protection of PII; and – Physical safeguarding measures for individual workspaces are adequate for the protection of PII. • Identify and report any security vulnerabilities in their assigned area to the Privacy Officer or PSA Privacy Point of Contact (PSA POC). • Ensure resources are appropriately requested and applied to identify, evaluate, and mitigate privacy risks. • Liaise with the Agencies' Privacy Officer or PSA POC to periodically review PII holdings to determine if continued collection is necessary and appropriate.

Continued on next page

Roles and Responsibilities, Continued

CSOSA Office of Procurement/ PSA Office of Finance and Administration	• Ensures that all contracts and other agreements include provisions requiring contractors and subcontractors to follow the Agencies' policies and procedures for protecting PII. • Initiates appropriate corrective action against a contractor for failure to follow the Agencies' policies and procedures for protecting PII.
PSA Privacy Point of Contact (PSA POC)	• Administers the day-to-day activities and responsibilities of privacy at PSA. • Assists in developing new or revised PSA SORNs. • Coordinates with CSOSA to publish PSA SORNs to the Federal Register. • Evaluates PSA data collection and coordinates with CSOSA to develop PIAs. • Investigates suspected or confirmed PSA privacy incidents to support Agencies' breach response. • Delivers annual privacy awareness training for PSA employees, contractors, and interns.
Privacy Officer	• Coordinates with PSA POC to manage the Agencies' information privacy protections and full compliance with the Privacy Act and applicable laws, regulations, and policies. • Develops and implements the Agencies' privacy policies and procedures, and initiates revisions based on updates from OMB, changes in regulations, changes in roles and responsibilities, etc. • Advises and trains program and system managers to ensure all privacy-related statutory, regulatory, and Agencies requirements are met. • Assists in developing new or revised SORNs, and publishes Federal Register notices for systems of records. • Develops and maintains PIA templates for Agencies' systems of records. • Evaluates completed PIAs to ensure they meet Privacy Act requirements. • Performs various administrative functions related to the Agencies' privacy program (e.g., submits reports to OMB, maintains Privacy Act records, reviews forms and other data collection instruments, etc.). • Coordinates the Agencies' response to all suspected and confirmed privacy incidents consistent with the Agencies' Breach Response Plan.

Continued on next page

Roles and Responsibilities, Continued

Privacy Officer, continued

- Develops and implements an annual privacy awareness training program for employees, contractors, and interns.

Senior Agency Official for Privacy (SAOP)

- Leads the Agencies' implementation of information privacy protections and full compliance with the Privacy Act and applicable laws, regulations, and policies.
- Designates the Agencies' Privacy Officer.
- Establishes and maintains privacy policies and procedures that are comprehensive, compliant, and current with updates from OMB, changes in regulations, changes in roles and responsibilities, etc.
- Approves and signs respectively CSOSA's and PSA's SORNs for publication in the Federal Register.
- Approves new or revised system of records.
- Manages privacy risks associated with agency activities that involve the creation, collection, use, processing, storage, maintenance, dissemination, disclosure, and disposal of PII by programs and information systems.
- Ensures the Agencies consider and address privacy implications of all agency policies and procedures at the earliest planning and development stages and throughout the lifecycle of the programs or information systems.
- Ensures the Agencies conduct periodic information privacy compliance reviews to promptly identify deficiencies, weaknesses, or risks and take action to remedy identified compliance issues.
- Participates in assessing the impact of technology on the privacy of personal information.
- Liaises with the Chief Information Officer (CIO) and Chief Information Security Officer (CISO) to reduce the exposure of PII in the Agencies' information systems and in the conduct of Agencies' business, and to reduce PII holdings whenever possible.
- Collaborates with the CIO and CISO to establish and maintain the Agencies' Breach Response Plan.

Continued on next page

Roles and Responsibilities, Continued

Senior Agency Official for Privacy (SAOP), continued	• Submits an annual SAOP privacy report to the OMB and other privacy-related reports, as required. • Ensures that employees, contractors, and interns receive appropriate training and education regarding their privacy protection responsibilities.
Office of General Counsel	• Interprets and provides legal advice on the Privacy Act and other privacy-related regulations, statutes, and requirements. • Assists program and system managers in determining the applicable statute or regulation for a new or revised system of records; • Reviews Privacy Act notices for applicable legal citations, routine uses, and other legal aspect of establishing or revising the system; • Advises management on appropriate actions involving the Agencies' systems of records, including release of information, appropriate use of information, and appeals (e.g., denials of Privacy Act information, denial of a request for correction or amendment of a record pursuant to the Privacy Act). • Coordinates with the CIO, CISO, SAOP, Privacy Officer, and PSA POC to minimize the risk of loss, unauthorized access, or other misuse of PII and ensure the proper interpretation and implementation of legal requirements.
CSOSA Director	Appoints an SAOP accountable for developing, implementing, and maintaining an agency-wide governance and privacy program to ensure compliance with all applicable laws and regulations regarding the collection, use, maintenance, sharing, and disposal of PII by programs and information systems.