

Corporation for National and Community Service

Policies and Procedures

Policy Number: 153

Effective Date: May 11, 2016

Revision Number: NA

Subject: Privacy Policy

Purpose: This policy describes the organizational controls for protecting privacy and Personally Identifiable Information (PII) within CNCS systems and to establish the proper handling of information requests received by CNCS to which the Privacy Act of 1974 applies ensuring CNCS compliance with the related statutory and regulatory requirements.

Who is Covered: Agency employees and contract personnel, and information systems under written agreement between the user or contract personnel and CNCS. All CNCS employees and contractors who receive requests to release personal or financial information maintained by CNCS.

Policies Replaced: Privacy section of Policy 376 Information Assurance and policy 153 – Requests to Release Personal or Financial Information under the Privacy Act

Originating Office: Office of Information Technology (OIT)

Approved By:



Asim Mishra
Chief of Staff

If you need this document in an alternative format, please contact the Administrative Services Help Desk at 202/606-7504 (voice) or 800-833-3722 (TDD).

Table of Contents

1.0	PRIVACY POLICY AND PROCEDURES	3
1.1.	Purpose of this Guide	3
1.2.	Privacy Terms	3
2.0	PRIVACY PROGRAM RESPONSIBILITIES	6
2.1.	Senior Agency Official for Privacy (SAOP)	6
2.2.	CNCS Chief Privacy Officer	6
2.3.	CNCS Privacy Act Officer	6
2.4.	Chief Information Officer (CIO)	6
2.5.	Heads of Operational Units	7
2.6.	Program Directors	7
2.7.	Program Managers	8
2.8.	System Developers/Designers	8
2.9.	Office of General Counsel	8
2.10.	Office of Procurement Services	9
2.11.	CNCS Office of Management and Budget Office of Information and Regulatory Affairs (OIRA) Coordinator	9
2.12.	Data Integrity Board	9
2.13.	Supervisors and CNCS Employees	10
2.14.	Vendors/Contractors	10
3.0	CNCS PRIVACY ACT PROGRAM GUIDE	11
3.1.	Disclosure of Information	11
3.2.	Collection and Use of Information	12
3.3.	Solicitation of Information	13
3.4.	Collection of Social Security Numbers	13
3.5.	Information Accuracy	13
3.6.	Standards of Conduct on Personal Information	13
3.7.	Safeguarding Information	14
3.8.	Other Agencies' Records	14
3.9.	Establishing or Revising Privacy Act Systems of Records in CNCS	14
4.0	CNCS PRIVACY ACT PROCEDURES GUIDE	15

1.0 PRIVACY POLICY AND PROCEDURES

The Corporation for National and Community Service (CNCS) is committed to implementing and administering a Privacy Policy that protects CNCS employees and other individuals' personally identifiable information (PII) consistent with the principles of the Privacy Act of 1974, the E-Government Act of 2002, the Federal Records Act, and other applicable laws and regulations. This policy document is reviewed and updated annually, or as needed.

1.1 Purpose of this Guide

This guide contains the policies and procedures put in place by CNCS to protect the personal information of employees and other individuals on whom CNCS maintains PII to include all information systems of records under the Privacy Act.

The guide is designed as a source of information and guidance for:

- Managers and supervisors who use the records and/or manage Privacy Act systems and the information in the systems
- Vendors and contractors who provide support services for systems containing personal information
- Management officials who have responsibilities for carrying out functions under the Privacy Act

It explains the responsibilities of CNCS managers and supervisors that relate to their staff's personal information and the responsibilities of the CNCS employees and vendors or contractors who manage and operate the various systems of records in CNCS.

1.2 Privacy Terms

The terms in this part are defined to ensure consistency and common understanding when used in the context of the Privacy Act:

- **Agency:** Federal Government executive or military departments, corporations, other establishments in the Executive Branch, and regulatory agencies (5 U.S.C. 551(1) and 5 U.S.C. 552a (a)(1)). The Privacy Act applies only to Federal Government agencies. It does not cover State and local government agencies.
 - **Individual:** A citizen of the United States or a legal resident alien on whom CNCS maintains Privacy Act records. CNCS employees are considered individuals under the Act and have all the rights specified by the Act.
 - **Record:** Any item, collection, or grouping of information about an individual which contains the individual's name or other personal identifier such as number or symbol, fingerprint, voiceprint, or photograph. The information may relate to education, financial
-

transactions, medical conditions, employment, or criminal history collected in connection with an individual's interaction with CNCS.

- **System of records (SORN):** A group of records under CNCS' control from which information is retrieved by the name of an individual, or by any number, symbol, or other identifier assigned to that individual.
- **System of records notice:** A notice published in the Federal Register by CNCS for each new or revised system of records. The purpose of the notice is to allow public comment on the system before its implementation.
- **Routine use:** Disclosure of a record for the purpose for which it is intended.
- **Request for access:** A request by an individual to obtain or review his or her record or the information in the record.
- **Disclosure of information:** Providing a record or the information in a record to someone other than the individual of record.
- **Exempt records:** Records that may not be obtained by an individual because they are exempted under the Privacy Act.
- **Solicitation:** A request by an officer or employee of CNCS for an employee's personal information to be included in a system of records for a specified purpose.
- **Program manager:** The CNCS official who is responsible for a system of records and the information in it. This person is always cited in the Federal Register system of records notice.
- **Computer matching:** The computerized comparison of information between CNCS and an outside source to verify an individual's eligibility for Federal benefits or to recoup delinquent debts.
- **Information technology (IT) system** (also known as electronic information system): The equipment and software used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information.
- **Information in identifiable form:** Data within an IT system or online collection that permits the identity of an individual to whom the information applies to be reasonably inferred; information that identifies the individual by name or other unique identifier or by which an individual is identified in conjunction with other data elements such as gender, race, birth date, geographic indicator, and similar personal information. Information permitting the physical or online contacting of a specific individual is considered information in identifiable form.

- **Privacy Impact Assessment (PIA):** The process for evaluating privacy issues in an electronic information system, including examining the risks and effects of collecting, maintaining, and disseminating information in identifiable form, and identifying and evaluating protections and alternative processes to mitigate the impact to privacy of collecting such information. The process consists of gathering data on privacy issues from a project, identifying and resolving privacy risks, and obtaining approval from agency privacy and security officials. Completion of the PIA process results in the PIA Report.

2.0 PRIVACY PROGRAM RESPONSIBILITIES

This section describes the roles and responsibilities of key positions involved in administering CNCS' Privacy program. Some of the following positions may be held by the same individual if there is not an oversight function, and some may be held by more than one individual if there is a clear delineation of responsibility.

2.1. Senior Agency Official for Privacy (SAOP):

Has overall responsibility for establishing and overseeing the Privacy Act Program in CNCS and for ensuring CNCS' compliance with privacy laws, regulations and CNCS policy. Specific responsibilities include duties outlined in [OMB Memorandum 05-08](#).

2.2. CNCS Chief Privacy Officer

Is responsible for coordinating the implementation of Privacy Act Program requirements within CNCS and the duties outlined under [42 U.S.C. §2000ee-2\(a\)](#).

2.3. CNCS Privacy Act Officer

Is the individual delegated the authority to allow access to, the release of, or the withholding of records pursuant to an official Privacy Act request. The Privacy Act Officer is further delegated the authority to make the initial determination on all requests to amend records. The Privacy Act Officer:

- Receives requests for access to records
- Make decisions to grant or deny access to records and notifies the requestor of the decision
- Reviews requests for amendments or corrections to individual's records, makes initial determination regarding amendment of the record, carrying out procedures in 45 CFR 2508.15 regarding amending the record
- Maintain records of Privacy Act requests.

2.4. Chief Information Officer (CIO)

Responsible for implementing IT security management in CNCS, with overall responsibility for the CNCS IT Security Program and the IT Capital Planning Program, and for security policy on electronic privacy data. Specific responsibilities include:

- Fill the role of SAOP, unless another person is appointed specifically for the role
- Ensures the protection of electronic privacy

- Oversees security policy for privacy data
- Ensures review of Privacy Impact Assessments for information security considerations
- Ensures that Privacy Impact Assessments are part of CNCS' System Development Life Cycle Guidance for Information Technology

2.5. Heads of Operational Units

Responsible for ensuring that the systems of records under their jurisdiction meet the requirements of the Privacy Act and CNCS privacy and security policies and procedures. Specific responsibilities include:

- Approve the establishment of new systems of records and the revision of existing systems within their program or unit
- Review Privacy Act notices to be submitted to the Federal Register for new and revised systems of records
- Approve reports on Privacy Act activities upon request by the CNCS Privacy Act Officer
- Ensure that contractors performing services associated with systems of records (such as system development, maintenance, or operation) are subject to the provisions of the Privacy Act and security requirements
- Consult with legal counsel, their program managers, and Privacy Act program officials on the disposition of special cases involving release of information, or on resolving appeals

2.6. Program Directors

Responsible for ensuring that the systems of records in their program areas meet the requirements of the Privacy Act and security policy and regulations. Specific responsibilities include:

- Ensure that the program systems of records are necessary, relevant to the program, and authorized by statute, regulation, or Executive Order
- Identify the need for and proposing the establishment of new or revised systems of records to accomplish program mission or functions
- Propose the cancellation of outdated or obsolete systems of records
- Consult with OGC and Privacy Act program officials on the use and release of system information under special conditions or appeals
- Identify and propose for exemption the systems that meet nondisclosure criteria under the Privacy Act

- Ensure that all contractors providing program systems of records services follow Privacy Act and security requirements
- Appoint a program manager for each of their system of records
- Identify systems requiring Privacy Impact Assessments (PIAs), coordinating on developing the PIAs, and resolving any privacy issues

2.7. Program Managers

Responsible for implementing the requirements described in this guide. Specific responsibilities include:

- Periodically review their system of records for need, relevance, and purpose for existence, and proposing changes as needed to meet changing circumstances
- Periodically review the information in the system to make sure it's still necessary, relevant, complete, and up-to-date
- For a new or a revised system of records, coordinate with the Chief Privacy Officer on preparing a Privacy Act notice for publication in the Federal Register
- Develop an appropriate form or other data collection method for collecting Privacy Act information that includes a Privacy Act statement
- Collect information directly from the individual whenever possible
- Understand the approved uses for the system information
- Establish appropriate administrative, technical, and physical safeguards to ensure security and confidentiality of records
- Serve as the point of contact for the system

2.8. System Developers/Designers

Responsible for ensuring that the system design and specifications conform to privacy standards and requirements and that technical controls are in place for safeguarding personal information from unauthorized access. Specific responsibilities include establishing system protection controls (e.g., access, retrieval, storage, user restrictions).

2.9. Office of General Counsel

Responsible for providing legal advice and assistance on Privacy Act matters and CNCS systems of records. Specific responsibilities include:

- Assists program and system managers to determine the applicable statute or regulation for a new or revised system of records
- Reviews the Privacy Act notice for applicable legal citations, routine uses, and other legal aspects of establishing or revising the system
- Approves each notice for publication
- Advises management on appropriate actions involving CNCS systems of records, including release of information, appropriate use of information, and appeals
- Provides legal opinions on all Privacy Act issues as needed

2.10. Office of Procurement Services

Responsible for ensuring compliance with FAR requirements related to privacy.

2.11. CNCS Office of Management and Budget Office of Information and Regulatory Affairs (OIRA) Coordinator

Responsible for providing advice and assistance on designing forms for collecting system of records information and clears the forms with OIRA.

2.12. Data Integrity Board

Responsible for reviewing and approving all computer matching programs and activities. Specific responsibilities include:

- The review, approval, and maintenance of all written agreements for the receipt or disclosure by CNCS of Privacy Act records for computer matching programs, including pilot matches, to ensure compliance with the Privacy Act's requirements and relevant statutes, regulations, and guidelines, including a review of the benefits and costs of all computer matching programs.
- The annual review for continued justification of all matching programs in which CNCS has participated as either a source or recipient agency, including an assessment of the utility of the programs in terms of their costs and benefits.
- Compilation of an annual report to the Chief Executive Officer and the Office of Management and Budget on CNCS' computer matching activities.
- Providing interpretation and guidance to CNCS on computer matching programs, and reviewing related recordkeeping and disposal policies and practices.

2.13. Supervisors and CNCS Employees

Responsible for ensuring that the personal information they use in carrying out their official duties is protected according to Privacy Act and security requirements.

2.14. Vendors/Contractors

CNCS vendors and contractors are responsible for ensuring the privacy and security of data and data systems they design, develop, maintain, operate, or use is done consistent with applicable requirements.

3.0 CNCS PRIVACY ACT PROGRAM GUIDE

This section outlines how CNCS handles PII, through collection, safeguarding, and disclosure. CNCS will ensure that when a request for personal or financial information related to a current or former employee or national service participant is received by CNCS that the request is evaluated and that a response is made consistent with the Privacy Act of 1974, CNCS privacy rules and this policy. A copy of the Privacy Act is available at [5 U.S.C. § 522a](#) and CNCS' Privacy Act regulations are available at [45 C.F.R. §§ 2508.1 - .20](#).

The release of personal information maintained by CNCS is governed by the provisions of the Privacy Act of 1974 and its related regulations. In some cases, the provisions determine whether we can release any information at all. The Privacy Act guarantees individuals three primary rights:

- The right to see records about oneself, subject to the Privacy Act's exemptions;
- The right to amend a nonexempt record if it is inaccurate, irrelevant, untimely, or incomplete; and
- The right to sue the government for violations of the Privacy Act, such as permitting unauthorized individuals to read an individual's records.

3.1. Disclosure of Information

No information contained in a Privacy Act system of records may be disclosed in a manner that is inconsistent with the Privacy Act. Disclosure of information outside of CNCS usually requires the written consent of the individual.

The following table lists some of the most common types of requests received by CNCS and lists the appropriate actions and responses CNCS departments should take. (NOTE: If there are questions about a request, or the request is not addressed in the table below, contact CNCS' FOIA/Privacy Act Officer, by phone, (202)-606-6747, or by email, FOIA@cns.gov.)

Written Request From:	Seeking	Action	Response by:
Courts or government officials	Confirmation of a member's service for reasons other than employment-related verification	Forward to OGC.	OGC
Employers, banks, mortgage companies, universities, bar examiners	Confirmation of a member's service	Forward to National Service Hotline.	National Service Hotline
Employees, Employers, and others	Employee Information	Forward to OHC	OHC
IRS	Tax levy	Forward to OGC.	OGC
Member or Former National Service Participant	To dispute of information in their service record	Forward to OGC.	OGC
IRS	Member Tax Information	Notify OGC; Forward to	Trust

Written Request From:	Seeking	Action	Response by:
		the Trust.	
IRS	Tax clarification letter for 1099 recipient.	Process according to OGC-approved procedure and form letter (rev. Feb 2012).	Trust
First-party requests submitted with a Notarized Signature	Written verification of their employment or service.	Forward to National Service Hotline.	National Service Hotline
Third-party requests submitted without a signed release authorizing disclosure or reliance on a specific routine use.	Any information.	Notify OGC.	OGC
Educational and lending institutions	Member information that will allow them to post payment to the correct account	Notify OGC; forward to the Trust.	Trust
Educational and lending Institutions	Information to complete the check trace, refund, and cancellation process of Trust Payments.	Notify OGC; forward to the Trust	Trust
Educational institutions	Information regarding the history of payments made to them	Notify OGC; forward to the Trust.	Trust
Attorneys	Education Award payment information	Notify OGC; forward to the Trust.	OGC in coordination with Trust
Attorneys	Any information.	Forward to OGC.	OGC
Programs or Commissions	Education Award Usage (aggregated)	Notify OGC; forward to the Trust	Trust
Tax Preparers	Any member-specific information	Forward to OGC	OGC
Program auditors	Member information to allow them to complete A-133	Notify OGC; forward to the Trust	Trust
Relatives of a National Service Participant	Any information on the member in a non-emergency situation	Forward to OGC.	OGC
State or Federal Government	Garnishment	Forward to OGC	OGC
Party not listed on this table	Any information.	Forward to OGC.	Office designated by OGC.

3.2. Collection and Use of Information

Personal information used to determine rights, benefits, and privileges must be collected directly from the individual of record whenever possible, and used only for the purpose for which it is intended.

3.3. Solicitation of Information

When soliciting personal information from an individual or a third party, the following information must be included on the data collection form or other data collection instrument:

- The legal or regulatory authority for collecting the information
- Whether furnishing the information is voluntary or mandatory
- The purpose for which the information will be used
- The routine uses of the information
- The effect on the individual of not providing the information

3.4. Collection of Social Security Numbers

Do not collect Social Security Numbers (SSNs) unless statutory authority exists for collecting SSNs for record systems that use the SSN for identification purposes. SSNs will not be collected for systems without this specific authority.

3.5. Information Accuracy

CNCS will make all reasonable efforts to ensure that personal information provided by individuals is accurate and complete. Managers should endeavor to maintain information in the system that is relevant, necessary, and timely.

3.6. Standards of Conduct on Personal Information

CNCS employees have the duty to protect the security of personal information by making all reasonable efforts to:

- Ensure the accuracy, relevance, timeliness, and completeness of records
- Avoid any unauthorized disclosure, verbal or written, of records
- Ensure that no system of records is maintained without a Federal Register notice
- Only collect personal information when authorized
- Collect only the information needed to perform an authorized agency function
- Collect information directly from the individual whenever possible
- Maintain and use records with care to prevent any inadvertent disclosure of information

3.7. Safeguarding Information

System managers must establish physical, administrative, and technical safeguards for their systems of records. The safeguards must be intended to ensure the security and confidentiality of records, protect against possible threats or hazards, and permit access only to authorized persons.

Paper records should be placed in secured locations. Electronic systems should use passwords, identity verification, detection of break-in attempts, firewalls, encryption, and/or other security measures determined to be appropriate by the responsible system and program managers.

3.8. Other Agencies' Records

Where CNCS has either permanent or temporary custody of other agencies' records, system managers will coordinate with those agencies on any release or disclosure of information. Office of Personnel Management (OPM) records that are in CNCS' custody will be handled according to OPM's rules and procedures.

3.9. Establishing or Revising Privacy Act Systems of Records in CNCS

The establishment of a new Privacy Act system of records or revision of existing system of records generally follows these steps:

- 1) A program manager determines that a new or revised system needs to be established to carry out a program responsibility or improve a process.
- 2) The program manager prepares a proposal that describes and justifies the establishment or revision of the system.
- 3) The program manager sends the proposal to the Chief Privacy Officer, OIT, and OGC, who consult with the program manager on the proposal and suggest revisions to the proposal, as necessary.
- 4) When the Chief Privacy Officer, OIT, program manager and OGC collaboration is complete, the team works to prepare the required documentation required under privacy laws and regulations to establish the new or revised system of records and submits the documentation for clearance and then to the necessary outside parties (OMB, Congress) and prepares the Federal Register documents for public notice and comment.

4.0 CNCS PRIVACY ACT PROCEDURES GUIDE

CNCS' Privacy Act Implementation regulations can be found at 45 CFR Part 2508. These regulations include how an individual may access his/her records, fees, conditions for denial of records, procedures for amending records, how an individual may appeal a refusal to amend a record, and other related procedures.