Corporation for National and Community Service

Policies and Procedures

Policy Number: 153 **Effective Date:** September 7 2017

Revision Number: NA

Subject: Privacy Policy

Purpose: This policy describes and sets forth the organizational controls for collecting, transmitting, storing and protecting Personally Identifiable Information (PII) within CNCS information systems and to establish the proper handling of information in accordance to the Privacy Act of 1974, as amended, and other applicable Federal statutes, regulations and Office of Management and Budget (OMB) directives.

Who is Covered: Agency employees, interns, volunteers, and contract personnel whom have access to CNCS systems that contain personal or financial information.

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

Table of Contents

1.0 PRIVACY POLICY AND PROCEDURES 4

1.1. Purpose 4

1.3. Privacy Terms 5

2.0 PRIVACY PROGRAM RESPONSIBILITIES 8

2.1. Senior Agency Official for Privacy (SAOP): 8

2.2. CNCS Chief Privacy Officer (PO) 8

2.3. Executive Team 9

2.4. Program Directors 9

2.5. Program Managers 9

2.6. System Developers/Designers 10

2.7. Office of General Counsel 10

2.8. Office of Procurement Services 11

2.9. CNCS Office of Management and Budget Office of Information and Regulatory Affairs (OIRA) Coordinator 11

2.10. Data Integrity Board 11

2.11. Supervisors and CNCS Employees 11

2.12. Vendors/Contractors 11

3.0 PRIVACY PROGRAM 12

3.1. Fair Information Practice Principles 12

3.2. Disclosure of Information 13

3.3. Production of Records for Court Proceedings 15

3.4. Disclosure of Records to Third Parties 16

3.5. Vendors and Contractors 17

3.6. Collection and Use of Information 18

3.7. Solicitation of Information 18

3.8. Collection of Social Security Numbers 19

3.9. Information Accuracy 19

3.10. Standards of Conduct on Personal Information 19

3.11. Safeguarding Information 20

3.12. Training 20

3.13. Other Agencies' Records 20
3.14. Establishing or Revising Privacy Act Systems of Records in CNCS 20
4.0 BREACH OF PII 22
4.1. CNCS Response 22
4.2. Contractor Response 23
4.3. Grants and Grantee Compliance and Response 24
4.4. Reporting Requirements 24
4.5. Tracking and Documenting Breach Responses 24
5.0 CNCS PRIVACY ACT PROCEDURES GUIDE 25

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, as amended ("The Privacy Act") at Title 5 United States Code (U.S.C.) 552a, Section 208 of the E-Government Act of 2002, OMB Circular A-130 (July 2016), the Federal Records Act of 1950, as amended 44 U.S.C. Chapter 31 and other applicable Federal laws, regulations and government-wide policy.

Federal law requires the Agency to inform employees and the public how the Agency collects, uses, shares, and protects personal information. Federal law also limits how the Agency can use an employee's or members of the public, personal information.

Specifically, the Privacy Act was enacted to safeguard individual privacy contained in federal records and to provide individuals access to records concerning them that are maintained by federal agencies. It safeguards privacy through creating four procedural and substantive rights in personal data. It requires Federal agencies to: 1) show an individual any records retained on him or her; 2) follow certain principles called "fair information practices," when gathering and handling personal data; 3) place restrictions on how agencies can share an individual's data with other people and agencies, and 4) it permits individuals legal remedies if the government violates the Privacy Act provisions.

The Privacy Act prohibits the disclosure of any record in a system of records by any means of communication to any person or agency absent the written consent of the individual, unless the disclosure falls within one of twelve (12) statutory exceptions identified in the Privacy Act.

This policy document is reviewed and updated annually, or as needed.

1.1. Purpose

The purpose of this policy is to help ensure compliance with privacy requirements and protect the personal information of employees and other individuals whom CNCS maintains PII for information collected, used, retained, and/or disseminated by the agency under the Privacy Act, and other applicable Federal laws, regulations and policies. This policy is intended to protect the security and integrity of the agency's data and technology infrastructure. Limited exceptions to the policy may occur due to variations in sensitive data, devices and platforms.

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

- Managers and supervisors who use information and/or manage CNCS systems that contain PII
- Vendors and contractors who provide support services for CNCS systems containing PII
- Management officials who have responsibilities for carrying out functions under the Privacy Act or any other mandate that requires the use of PII

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 Authority

The Privacy Act provides statutory privacy rights to U.S. citizens and legal permanent residents. The Agency follows the requirements of the Privacy Act which protects personal information that the Agency maintains in systems of records (SORs). A system of records is a file, database, or program from which personal information is retrieved by name or other personal identifier. A list of the authorities and references are listed in Attachment A.

1.3. Privacy Terms

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

- **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.

- **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.

- **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.

- **Fair Information Practice Principles (FIPPs)**: a collection of widely accepted principles that CNCS will use when evaluating information systems, processes, programs, and activities that affect individual privacy.

- **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.

- **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.

- **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.

- **Personally Identifiable Information (PII):** Is information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual.

- **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.

- **Privacy Threshold Assessment (PTA)**: The PTA is an administrative form to identify and assess the use of PII in CNCS systems across agency business units.

- **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.

- **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.

- **Request for access**: A request by an individual to obtain or review his or her record or the information in the record.

- **Routine use**: Disclosure of a record for the purpose for which it is compatible and for which it is collected.

- **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.

- **System of records**: 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 (SORN)**: The notice(s) published by CNCS in the Federal Register upon the establishment and/or modification of a system of records describing the existence and character of the system. A SORN identifies the system of records, the purpose(s) of the system, the authority for maintenance of the records, the categories of records maintained in the system, the categories of individuals about whom records are maintained, the routine uses to which the

records are subject, and additional details about the system as described in OMB Circular A-108, Federal Agency Responsibilities for Review, Reporting, and Publication under the Privacy Act. The purpose of a SORN is to foster agency accountability in accordance with the Privacy Act.

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):

The SAOP has agency-wide responsibility and accountability for developing, implementing, and maintaining an agency-wide privacy program to ensure compliance with all applicable statutes, regulations, and policies regarding the creation, collection, use, processing, storage, maintenance, dissemination, disclosure, and disposal of PII by programs and information systems, developing and evaluating privacy policy, and managing privacy risks at the agency. Specific responsibilities include duties outlined in OMB Circular A-130, Appendix I.

2.2. CNCS Chief Privacy Officer (PO)

The PO 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). The PO shall also work in conjunction with the Chief Information Officer (CIO) to ensure that privacy is addressed throughout the life cycle of each information system and proper protections are in place for electronic PII by conducting a Privacy Threshold Assessment (PTA) and/or Privacy Impact Assessment (PIA). The PO is also responsible for ensuring that a system of records notice is published with the Federal Register for each system that collects PII.

The PO or designated representative:

- Receives requests for access to records
- Approves access to, the release of, or the withholding of records pursuant to an official Privacy Act request
- Makes the initial determination on all requests to amend 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 in accordance with NARA records schedule

2.3. Executive Team

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 PO
- 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

2.4. 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

2.5. Program Managers

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

- Periodically review their system of records for need, relevance, and purpose for existence, and propose 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 information collected
- Establish appropriate administrative, technical, and physical safeguards to ensure security and confidentiality of records
- Serve as the point of contact for the system

2.6. 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).

2.7. 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

2.8. Office of Procurement Services

Responsible for ensuring compliance with the Federal Acquisition Regulation (FAR) requirements related to privacy.

2.9. 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, clears the forms with OIRA and ensures that the agency is compliant with the Paperwork Reduction Act of 1995.

2.10. 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.

2.11. 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.

2.12. Vendors/Contractors

CNCS vendors and contractors are responsible for ensuring the privacy and security of data and data systems that they design, develop, maintain, operate, or use is done consistent with applicable requirements. Contractors must follow applicable sections of OMB Memorandum M-17-12, Preparing for and Responding to a Breach of Personally Identifiable Information (PII).

3.0 PRIVACY PROGRAM

This section outlines how CNCS handles PII, through collection, safeguarding, use, 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 properly evaluated and a response is provided that is 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.

All agency personnel, personnel providing information technology services to the agency, private contractors, and users must comply with all applicable laws protecting privacy in the collection, use, analysis, retention, destruction, sharing, and disclosure of information. Information retained by the agency may be disseminated to individuals in the public or private entities only for performance of official duties, public protection, safety or public health purposes in accordance with applicable laws and procedures.

3.1. Fair Information Practice Principles

The Fair Information Practice Principles (FIPPs) form the basis of CNCS' privacy compliance policies and procedures governing the use of personally identifiable information (PII). The FIPPs are used a guideline when reviewing privacy sensitive systems, programs, and information sharing arrangements and are derived from the Privacy Act and other federal and international privacy guidelines.

1. Access and Amendment – CNCS will provide individuals with appropriate access to PII and provide them the opportunity to correct or amend that information.
2. Accountability – CNCS will ensure compliance with the FIPPs and all other privacy requirements.
3. Authority – CNCS will only create, collect, use, process, store, maintain, disseminate, or disclose PII under proper authority.

4. Minimization – CNCS will only create, collect, use, process, store, maintain, disseminate or disclose PII that is directly relevant and necessary to accomplish a legally authorized purpose and should only maintain PII for as long as is necessary to accomplish the purpose.

5. Quality and Integrity - CNCS should create, collect, use, process, store, maintain, disseminate, or disclose PII with such accuracy, relevance, timeliness, and completeness as is reasonably necessary to ensure fairness to the individual.

6. Individual Participation – CNCS will only involve the individual in the process of using PII and, to the extent practicable, seek individual consent for the creation, collection, use, processing, storage, maintenance, dissemination, or disclosure of PII. CNCS will establish procedures to receive and address individuals' privacy-related complaints and inquiries.

7. Purpose Specification and Use Limitation – CNCS will provide notice of the specific purpose for which PII is collected and should only use, process, store, maintain, disseminate, or disclose PII for a purpose that is explained in the notice and is compatible with the purpose for which the PII was collected, or that is otherwise legally authorized.

8. Security - CNCS will establish administrative, technical, and physical safeguards to protect PII commensurate with the risk and magnitude of the harm that would result from its unauthorized access, use, modification, loss, destruction, dissemination, or disclosure.

9. Transparency - CNCS will be transparent about information policies and practices with respect to PII, and should provide clear and accessible notice regarding creation, collection, use, processing, storage, maintenance, dissemination, and disclosure of PII.

3.2. 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 or other applicable requirements. Disclosure of information outside of CNCS usually requires the written consent of the individual, unless it comes within one of the twelve exceptions of the Privacy Act or other federally mandated requirements.

CNCS will ensure that information gathered and retained by this agency will be disclosed to a member of the public only if the information complies with the Privacy Act and/or any other applicable law or policy setting forth public access to information. The agency will collect and use only the minimum information necessary to accomplish Agency mission related functions and operations. Electronically submitted information is maintained and destroyed according to the principles of the Federal Records Act and the regulations and records schedules of the National Archives and Records Administration and in some cases may be covered by the Privacy Act and subject to the Freedom of Information Act (FOIA).

Agency personnel and contractors will release an agency record in response to a written request in accordance to the requirements of this policy, unless a valid legal exemption to disclosure applies. The primary responsibility for the operation of the Agency information system including operations, coordination of personnel, the receiving, seeking, retention, evaluation, information quality, systems, including operations, coordination of personnel, the receiving, seeking, retention,

evaluation, information, analysis, destruction, sharing and disclosure of information, and the enforcement of this policy is assigned to the Privacy Officer.

CNCS or its contractors shall not confirm the existence or nonexistence of information to any person or agency that would not be eligible to receive the information based on applicable law or policy. An audit trail will be kept of all requests and of what information is disclosed to a member of the public.

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 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 the Trust.	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

Written Request From:	**Seeking**	**Action**	**Response by**:
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.

3.3. Production of Records for Court Proceedings

Agency records may be sought by subpoena, court order, or other court demand in connection with court proceedings to which the Agency is not a party. Records or testimony concerning CNCS may not be produced in court without the written approval of the General Counsel or designee. Records or testimony concerning CNCS may not be produced in court without the approval of CNCS's General Counsel or designee.

CNCS personnel who receive a subpoena, court order or other court demand shall forward the documentation to the Office of the General Counsel for processing.

3.4. Disclosure of Records to Third Parties

1. It is imperative that Agency employees maintain and process all information concerning individuals in a manner that ensures that information is accurate, relevant, and timely, and to ensure that no inadvertent disclosure of information is made.

2. Information that concerns an individual and that is contained in a system of records maintained by the Agency shall not be disclosed to any person, or to another agency, except under the provisions of the Privacy Act or the Freedom of Information Act or pursuant to a routine use under a SORN.

3. Personnel may disclose information from an Agency system of records once it has been reviewed by OGC, only if one or more of the following criteria apply:

    a) The Agency employee has obtained and submitted the written consent of the individual to whom the record pertains to the appropriate office or designated person.

    b) The record is needed by Agency employees in the performance of their official duties.

    c) If disclosure is permitted under FOIA, e.g. "public information," when the public interest in disclosure of the information outweighs the privacy interest involved.

    d) For a routine use described in the agency's system of records notice (SORN) published in the Federal Register. A "routine use" is defined by the Privacy Act as a "use…for a purpose which is compatible with the purpose of which [the record] was collected," and permits an agency to disclose a record without the consent of the subject to certain identified recipients.

    e) If another exception other than routine use as defined by the Privacy Act permits the disclosure.

    f) The Health Insurance Portability and Accountability Act of 1996 (HIPAA) permits the disclosure of Protected Health Information ("PHI") to law enforcement officials in specified circumstances:

        a. Pursuant to legal process and as otherwise required by law;

        b. To a limited degree, for purposes of identifying and locating certain classes of persons;

        c. As necessary to alert law enforcement to the commission and circumstances of a crime, and

d. "Law enforcement" is broadly conceived by HIPAA. It includes any governmental agency or official authorized to investigate, prosecute or conduct an inquiry into a potential violation of law.

4. The confidentiality of alcohol and drug abuse records maintained by the Agency is protected by Federal law and regulations. 42 U.S.C. 290dd–3 and 42 U.S.C. 290ee–3 and 42 CFR part 2. Generally, the Agency may not say to a person outside of the agency that an employee or member attends a drug or alcohol treatment program, or disclose any information identifying an employee or member as an alcohol or drug abuser unless, the employee or member consents in writing or:

   a. The disclosure is allowed by a court order;

   b. The disclosure is made to medical personnel in a medical emergency or to qualified personnel for research, audit, or program evaluation, or

   c. There are some situations in which the Agency is legally obligated to take actions as necessary to attempt to protect others from harm.

5. The published SORNs for Privacy Act-protected systems of records describe the contents of each system, methods of retrieving, and the routine uses for disclosing these records without first obtaining the consent of the person to whom the records pertain.

6. When emailing sensitive PII outside of the Agency, save it in a separate document and password-protect or encrypt it. Send the encrypted document as an email attachment and provide the password to the recipient in a separate email or by phone. Some components require encryption when emailing Sensitive PII within the Agency.

7. Never email sensitive PII to a personal email account. If you need to work on Sensitive PII off site use an agency-approved encrypted USB flash drive.

8. Protect hard copy sensitive PII: Do not leave Sensitive PII unattended on desks, printers, fax machines, or copiers. Secure sensitive PII in a locked desk drawer, file cabinet, or similar locked enclosure when not in use. When using sensitive PII, keep it in an area where access is controlled and limited to persons with an official need to know. Avoid faxing sensitive PII, if at all possible, unless the recipient has been notified to wait by the fax machine to receive the fax.

3.5. Vendors and Contractors

Vendors/Contractors are subject to the same laws and regulations as Federal employees and are therefore responsible for ensuring the privacy and security of systems they design, develop, maintain, operate, or use and for system data. They are accountable for any violation

that may occur due to oversight or negligence and may be subject to civil or criminal penalties under the Privacy Act.

3.6. 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.

These rules describe how and where data should be safely stored. Questions about storing data safely can be directed to the IT manager or data controller.

When data is stored on paper, it should be kept in a secure place where unauthorized people cannot see it.

These guidelines also apply to data that is usually stored electronically, but has been printed out for some reason:

- When not required, the paper or files should be kept in a locked drawer or filing cabinet.
- Employees should make sure paper and printouts are not left where unauthorized people could see them, e.g. a printer.
- Data printouts should be shredded and disposed of securely when no longer required.
- When data is stored electronically, it must be protected from unauthorized access, accidental deletion and malicious hacking attempts.
- Data should be protected by strong passwords that are changed regularly and never shared between employees.
- If data is stored on removable media (e.g. a CD or DVD), these should be kept locked away securely when not being used.
- Data should only be stored on designated drives and servers, and should only be uploaded to an approved cloud computing services.
- Servers containing personal data should be sited in a secure location, away from general office space.
- Data should be backed up frequently. Those backups should be tested regularly, in line with the agency's standard backup procedures.
- Data should never be saved directly to laptops or other mobile devices like smart phones.
- All servers and computers containing data should be protected by approved security software and a firewall.

3.7. 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 for not providing the information

3.8. 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 the specific authority from the Chief Privacy Officer.

3.9. 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.

3.10. 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
- Non-compliance with the Privacy Act carries criminal and civil penalties or disciplinary actions where appropriate

An employee may be liable if he or she knowingly and willfully

a. obtains or requests records under false pretenses,
b. discloses privacy data to any person not entitled to access, or
c. maintains a “system of records” without meeting Federal Register notice requirements.

3.11. 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.

3.12. Training

Agency employees must receive annual training on privacy and data protection policies and procedures. The training program will include, but not limited to:

- Purposes of the privacy protection policy;
- Substance and intent of the provisions of the policy relating to collecting use; analysis retention, destruction, sharing and disclosure of information retained by the agency;
- The impact of improper activities associated with information accessible within or through the agency, and
- The nature and possible penalties for policy violations including possible transfer dismissal, civil and criminal liability, and immunity, if any.

3.13. 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.

3.14. 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 BREACH OF PII

PII regardless of whether it is in paper or electronic form, must be protected from unauthorized access or disclosure throughout its lifecycle, and agency personnel shall limit the use of PII to only that information which is specifically needed to carry out their duties. Employees are required to prevent the unauthorized use of PII. Upon a finding of a suspected or confirmed data breach involving PII in printed or electronic form, personnel must immediately report the incident to the CISO in accordance with existing cyber incident reporting processes.

In accordance with OMB M-17-12 a breach is defined as:

"The loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or any similar occurrence where (1) a person other than an authorized user accesses or potentially accesses personally identifiable information or (2) an authorized user accesses or potentially accesses personally identifiable information for an other than authorized purpose."

A breach is not limited to an occurrence where a person other than an authorized user potentially accesses PII by means of a network intrusion, a targeted attack that exploits website vulnerabilities, or an attack executed through an email message or attachment. A breach may also include the loss or theft of physical documents that include PII and portable electronic storage media that store PII, the inadvertent disclosure of PII on a public website, or an oral disclosure of PII to a person who is not authorized to receive that information.

Types of breaches that must be reported include, but are not limited to the following:

a. loss of control of employee or supervisee information consisting of names and Social Security numbers;
b. loss of control of agency credit card holder information;
c. loss of control of PII pertaining to the public;
d. loss of control of security information (e.g., logons, passwords, etc.);
e. incorrect delivery of PII;
f. theft of PII, and
g. unauthorized access to PII stored on Agency operated websites.

4.1. CNCS Response

CNCS will take all necessary actions when:

1. CNCS suspects or has confirmed that there has been a breach of the system of records

2. CNCS has determined that as a result of the suspected or confirmed breach there is a risk of harm to individuals, CNCS (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 CNCS' efforts to respond to the suspected or confirmed breach or to prevent, minimize, or remedy such harm.

4. CNCS has determined that information from its system of records is reasonably necessary to assist the recipient agency or entity in responding to a suspected or confirmed breach or 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.

5. CNCS will notify an individual about whom unencrypted personal information was or is reasonably believed to have been obtained by an unauthorized person and access to which threatens physical or financial harm to the person. The notice will be made promptly and without unreasonable delay following discovery or notification of the access to the information and consistent with the Agency's Breach Notification Policy. The Agency will conduct an internal investigation on the release or take any measures necessary to determine the scope of the release of information and to reasonably restore the integrity of the information system.

4.2. Contractor Response

All CNCS contracts shall have the baseline privacy clauses that include the minimum requirements under NIST Special Publication 800-171--Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations and the required privacy FAR clauses. As such, a CNCS contractor must provide at least the following in response to a breach of PII:

- Contractors and subcontractors (at any tier) are required to report a suspected or confirmed breach in any medium or form, including paper, oral, and electronic, as soon as possible and without unreasonable delay, consistent with the agency's incident management policy and US-CERT notification guidelines;

- Contractors and subcontractors (at any tier) are required to maintain capabilities to determine what Federal information was or could have been accessed and by whom, construct a timeline of user activity, determine methods and techniques used to access Federal information, and identify the initial attack vector;
- Allow for an inspection, investigation, forensic analysis, and any other action necessary to ensure compliance with this Memorandum, the agency's breach response plan, and to assist with responding to a breach;

- As directed by CNCS notify any individuals potentially affected by a breach, take countermeasure to mitigate the risk of harm to potentially affected individuals or to protect PII on behalf of the agency, including operating call centers and providing resources;

- Accounting of disclosures to third parties must be made in accordance with Agency policy. Except for disclosures of information to other Agency employees and disclosures required under the FOIA, an accounting of disclosure to third parties of any information concerning an individual contained in an Agency system of records will be made in accordance with Agency policy.

4.3. Grants and Grantee Compliance and Response

CNCS grantees must also protect CNCS data in accordance to NIST Special Publication 800-171--Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations. They must have procedures in place to response to a breach that at a minimum include timely notification to CNCS.

4.4. Reporting Requirements

CNCS will follow OMB M-17-12 and any other applicable CNCS documentation when reporting on a suspected or confirmed breach of PII.

4.5. Tracking and Documenting Breach Responses

CNCS will use the Breach Reporting Form [1]to record any suspected breaches of PII. Information gathered from the form will assist in documenting:

- The total number of breaches reported over a given period of time
- The status for each reported breach, including whether the agency's response to a breach is ongoing or has concluded
- The number of individuals potentially affected by each reported breach
- The types of information potentially compromised by each reported breach
- Whether the agency, after assessing the risk of harm, provided notification to the individuals potentially affected by a breach
- Whether the agency, after considering how best to mitigate the identified risks, provided services to the individuals potentially affected by a breach
- Whether a breach was reported to US-CERT and/or Congress.

[1] Breach Reporting Form is located at https://nationalservice.gov/privacy

5.0 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.