



Corporation for National & Community Service Policies and Procedures

Policy Number: CIO 2008-001

Effective Date: September 15, 2008

Revision Number: 0

Subject: Information Privacy Policies

1. Purpose: The Privacy Act of 1974, Federal Information Security Management Act of 2002, OMB guidance, and other federal regulations require the Corporation to establish a fully integrated information privacy program to ensure that information on individuals that is collected and used by CNCS is appropriately handled and protected. This document describes the policies and procedures that CNCS will implement to appropriately safeguard sensitive personal information and implement CNCS' Information Privacy Program in accordance with statutory and regulatory requirements. The policies and procedures described in this document will be supplemented by a series of directives, standards, and other guidance documents that address specific aspects of the information privacy program.
2. Who is Covered: All persons who have access to or use Corporation information resources
3. Policies Cancelled: N/A
4. Originating Office: Office of Information Technology.
5. Location of Revised Text: New document
6. Attachments:
 - a. CNCS Information Privacy Policies
 - b. CNCS Information Privacy Program (IPP) Handbook

Corporation employees can access this document electronically at intranet.cns.gov

Approved By:

[signed version on file with CEO and CIO]

Nicola Goren, 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 202/565-2799 (TTY). You may also send an e-mail to ashelp@cns.gov or write: Corporation for National Service, Office of Administrative and Management Services, 1201 New York Avenue N.W., Washington D.C. 20525.

1. What does this document do?

This document provides Corporation staff with guidance about information privacy policies. These policies ensure that CNCS properly collects, handles, and protects personal information about individuals. Federal laws and regulations require us to have these policies.

You must comply with this policy if you have access to any information (electronic or paper) at or on behalf of the Corporation.

2. Policy Transition Schedule

To provide an adequate transition period to familiarize existing staff with the new information privacy policies, CNCS has established the following policy implementation schedule:

- Existing staff (including employees, contractors, interns, etc.) will have 30 days from policy issuance to familiarize themselves with the policies. Enforcement of new policy provisions that were not previously in force at CNCS will commence upon completion of this period. Pre-existing policy provisions and any policies involving illegal activity will be enforced during this 30 day period.
- New personnel who join the Corporation after the issuance of the policies will be required to comply with all policy provisions as of the effective date of the policy. Privacy training will be incorporated into the new staff orientation process.

3. Training Plan

Training sessions will be provided prior to the policy effective date to provide an overview of the new policies and the privacy program.



Corporation for National & Community Service
Office of Information Technology

INFORMATION PRIVACY
POLICIES

August 2008

TABLE OF CONTENTS

A. INTRODUCTION	2
B. OBJECTIVES	2
C. SCOPE	3
D. GUIDING PRINCIPLES	3
E. REQUIREMENTS	4
E.1 Federal Government Requirements.....	4
E.2 Business and Operation Concerns.....	5
E.3 Protecting Individuals	7
F. POLICY FRAMEWORK	10
F.1 Relationship to Information Security Program	10
F.2 Policy Numbering	11
F.3 Policy Structure.....	11
G. INFORMATION PRIVACY ROLES AND RESPONSIBILITIES	12
G.1 General Information Privacy Roles.....	12
G.2 Designated Roles	14
H. POLICIES	22
APPENDIX A: FEDERAL REQUIREMENTS AND GUIDANCE	23
APPENDIX B: ACRONYMS AND ABBREVIATIONS	31
APPENDIX C: INFORMATION PRIVACY ROLE ASSIGNMENTS (AS OF APRIL 2008)	32
APPENDIX D: INFORMATION PRIVACY POLICY DOCUMENTS.....	33

A. INTRODUCTION

The Corporation for National and Community Service (CNCS) requires that individuals provide information about their lives, financial status, health status, and other activities in support of the Corporation's mission. This information may be required to support hiring actions for employees or to qualify for participation in various contract, grant, and volunteer activities. Individuals provide this information with the expectation that the Corporation will exercise due care to protect the information entrusted to them from unauthorized access and will use that information only for the purpose for which it was provided.

Recognizing the need for individuals to continue to voluntarily provide the government with their personal information, and the responsibility of the Government to protect this information, Congress and the Office of Management and Budget (OMB) enacted laws and regulations requiring that federal agencies establish Privacy Programs to monitor the collection of personal information and to protect that information once it has been collected.

The CNCS Information Privacy Program (IPP) has been designed to ensure that the Corporation is compliance with all federal privacy requirements and that the information collected and used by CNCS is appropriately handled and protected.

This information privacy policy document describes the policies and procedures that CNCS will implement to appropriately safeguard sensitive personal and business information and implement CNCS' Information Privacy Program in accordance with statutory and regulatory requirements. The policies and procedures described in this document will be supplemented by a series of directives, standards, and other guidance documents that address specific aspects of the privacy program.

B. OBJECTIVES

The purpose of this privacy policy document is to identify and disseminate the principles and framework that guide the safeguarding of sensitive personal and business information handled by the Corporation. The policies outlined in this document are based on existing federal requirements and standards as well as industry best practices.

Specifically, this document discusses:

- The principles on which the CNCS information privacy policies are based
- Federal regulations and standards with which CNCS must comply
- CNCS business-driven security requirements
- The information privacy policy framework to be used at CNCS
- The set of CNCS privacy policies to be implemented to appropriately safeguard sensitive personal and business information.

C. SCOPE

The policies in this document define the minimum set of requirements for protecting privacy information, including both Personally Identifiable Information (PII), and complying with applicable regulations.

CNCS information privacy policies apply to everyone who uses or has access to privacy information, both electronic and paper, including employees, contractors, customers, vendors, volunteers, and visitors regardless of time and locations. All of these personnel are responsible for understanding and complying with these policies.

The policies apply to the use of all privacy data collected or handled by, or on behalf of, the Corporation, regardless of time or location.

D. GUIDING PRINCIPLES

The development of CNCS' information privacy policies is driven by the following principles:

- CNCS must fully comply with all applicable regulations and federal guidelines regarding privacy.
- Privacy information maintained by the Corporation is reviewed regularly, to the maximum extent practicable, to ensure such information is accurate, relevant, timely, and complete.
- Only privacy information required to support CNCS' mission and business needs is maintained by the Corporation.
- CNCS is committed to protecting the private information entrusted to the Corporation by its customers and partners.
- Information privacy protection is the responsibility of all CNCS employees and can only be successfully achieved through communication and cooperation.
- CNCS will identify personnel with significant security and privacy responsibilities, and tailor training to support various roles and responsibilities commensurate with respective responsibilities and with any special requirements of their specific jobs.
- Information privacy is an essential component of sound IT management.
- A comprehensive and integrated approach is required to provide effective information privacy.
- CNCS' information privacy policies, procedures, and guidelines will be periodically reassessed to ensure continued effectiveness.

E. REQUIREMENTS

CNCS must protect customer information, employee data, and its own corporate assets as any corporation would, while also meeting federal government privacy mandates such as the Privacy Act of 1974, FISMA, OMB requirements, and presidential directives.

The CNCS Information Privacy policies must protect privacy data from three perspectives:

- Compliance with Laws and Federal Mandates
- Addressing business and operational privacy concerns (such as liability, reputation, and maintaining the confidence and cooperation of participants in its programs)
- Protecting the program participants from harm due to the Corporation's collection and use of their privacy information.

The following sections will discuss each of these sets of requirements. The combined set of these requirements forms the basis for CNCS' information privacy policies.

E.1 Federal Government Requirements

CNCS is subject to a variety of federal security requirements, including government regulations, federal standards, and the mandates of oversight agencies. These include, but are not limited to, the following, which are described in more detail in Appendix A:

- The Privacy Act of 1974
- The Computer Matching and Privacy Protection Act of 1988
- Computer Matching and Privacy Protection Amendments of 1990
- The Government Paperwork Reduction Act of 1995 (44 U.S.C. § 101 note) and the Information Technology Management Reform Act of 1996 (also known as Clinger-Cohen Act)
- Federal Information Security Management Act of 2002 (FISMA)
- Office of Management and Budget (OMB) Circular No. A-130, Transmittal No. 3, Appendix I, "Federal Agency Responsibilities for Maintaining Records About Individuals"
- OMB Circular A-123, "Management Accountability and Controls"
- Freedom of Information Act of 1996 (FOIA)
- Section 208 of the E-Government Act of 2002 (44 U.S.C. § 3501 note)
- Office of Management and Budget (OMB) Memoranda
- National Institute of Standards and Technology (NIST) Guidance
- Health Insurance Portability and Accountability Act of 1996 (HIPAA)

- 5 CFR part 293, “Personnel Records”
- Gramm-Leach-Bliley Act (GLBA)
- Fair Credit Reporting Act (FCRA)
- Children's Online Privacy Protection Act (COPPA)

E.2 Business and Operation Concerns

The purpose of federal privacy requirements is to balance the government's need to maintain information about individuals with the rights of individuals to be protected against unwarranted invasions of their privacy stemming from federal agencies' collection, maintenance, use, and disclosure of personal information about them. The Privacy Act of 1974 (5 U.S.C. § 552a) was enacted because Congress was concerned with curbing the illegal surveillance and investigation of individuals by federal agencies; it was also concerned with potential abuses presented by the government's increasing use of computers to store and retrieve personal data by means of a universal identifier – such as an individual's social security number.

CNCS collects personal information about employees, members, grantees, and other individuals for a variety of authorized purposes to deliver efficient and effective services. In order to fulfill its mission, the Corporation must protect this information. Failure to do so would not only result in loss of critical information, legal action, and increased government oversight, but also loss of confidence by the individuals whose information is needed. This loss of confidence could significantly compromise the Corporation's ability to successfully perform its mission.

E.2.a CNCS Business Environment

The Corporation for National and Community Service (CNCS) is an independent federal corporation. The Corporation has a Board of Directors and Chief Executive Officer appointed by the President and confirmed by the Senate. The Chief Executive Officer oversees the agency, which includes about 600 employees operating throughout the United States and its territories. CNCS is headquartered at 1201 New York Avenue, N.W. in Washington, D.C. which is a mixed use facility containing both federal government and commercial businesses.

CNCS was established in 1993 to connect Americans of all ages and backgrounds with opportunities to give back to their communities and their nation. The mission of CNCS is to improve lives, strengthen communities, and foster civic engagement through service and volunteering. CNCS provides grants and training and technical assistance to developing and expanding volunteer organizations. In addition, the Corporation explores, develops, and models effective approaches for using volunteers to meet the nation's human needs and conducts and disseminates research that helps develop and cultivate knowledge that will enhance the overall effectiveness of national and community service programs.

E.2.b Critical Information

CNCS has access to and maintains a variety of sensitive personal and business information, such as employee payroll and contact information, member social security numbers and medical histories, etc. This information is susceptible to theft and misuse. In addition to providing protection mandated by the Privacy Act, CNCS has an obligation to protect the information it requests from or creates about employees and other individuals. Threats to personal privacy may arise from both insiders and outsiders who wish to sell the information, use it to commit fraud, or simply satisfy curiosity.

CNCS information that must be protected from an Information Privacy perspective includes the following:

- **Member/Grantee Information** is collected and used to screen applicants, manage grants, operate programs, and carry out the Corporation's mission. Examples include: social security numbers, contact information, background investigations, medical data, etc.
- **Personnel Information** is necessary for CNCS to administer human resources programs, including compensation and benefits. Examples include payroll information; benefits information; retirement information; time and attendance information; and program information (*e.g.*, staffing, employee relations, etc.).
- **Financial Information** is essential for CNCS to carry out its financial functions and activities. Examples include accounts payable information, fixed assets, general ledger, grant information, budget and travel information.
- **Program and Legal Information** is essential for CNCS to carry out its programmatic and legal functions and activities and to protect the U.S. government and the legal and financial rights of CNCS' customers. Examples include client information; grant documentation; working documents; and FOIA information.

E.2.c Areas of Risk

The primary goal of the CNCS Information Privacy Program is to safeguard sensitive personal and business information to prevent its theft, loss, or compromise. Without a comprehensive privacy program, customized to CNCS' specific needs and environment, CNCS is exposed and vulnerable to losing its ability to perform its mission, and may risk liability for not protecting the resources with which it has been entrusted. CNCS faces a variety of Information Privacy threats, ranging from identity thieves to intentional employee misuse to accidental exposure of information. Each of these threats, when targeted at privacy information, can have a serious impact on the ability of CNCS to perform its mission. Table E-1 shows the potential harm or damage that could result from threats to CNCS' privacy information:

Table E-1: Potential Risks to CNCS Information

Critical Information Resource	Potential Harm or Damage
Member/Grantee Information	Financial/Legal Liability; Disclosure of Privacy Act information; Loss of Client Confidence; Inability to Perform Mission
Personnel Information	Financial/Legal Liability; Disclosure of Privacy Act protected information; Loss of Employee Confidence; Scrutiny by OPM
Financial Information	Financial loss; Loss of Assets; Disclosure of Sensitive Data; Inability to Perform Mission; Scrutiny by OMB and Congress
Program and Legal Information	Legal and Financial Liability; Disclosure of Sensitive Data; Loss of Client Confidence; Inability to Perform Mission

E.3 Protecting Individuals

“Privacy is the claim of individuals, groups or institutions to determine for themselves when, how, and to what extent information about them is communicated to others”¹. Individuals have a right against unsanctioned invasion of privacy by the government, corporations or individuals. However, privacy is not an absolute. “Each individual is continually engaged in a personal adjustment process in which he balances the desire for privacy with the desire for disclosure and communication.”²

Information privacy is the aspect of privacy that deals with an individual's expectations and rights regarding the confidentiality of data about themselves. Privacy concerns exist wherever data is uniquely identifiable to a specific person or persons, whether electronic or not. Concerns about data privacy arise in many areas from the confidentiality of data to how it is used. In order for the individual to make informed decisions about the privacy of their information, they must be given notice about the information that is collected about them, what it will be used for, who will have access to it, what choices they have regarding its collection and use, and what their rights are under the law.

When the information collected is used to make decisions about the individual, either directly or indirectly, such as when it affects credit worthiness, is used to make hiring decisions, or determines eligibility for a government program, issues also arise regarding the accuracy of the information. Individuals must have the right to access and request corrections to their data in order to ensure that they are being treated fairly.

CNCS' Information Privacy Program must address the whole range of these issues to ensure that individual's maintain the right to control the access and use of their data as well as be assured

¹ Alan Westin: Privacy & Freedom, 1967

² Alan Westin, 1967

that the data about them used by the government is correct. This includes not only protecting the confidentiality of personal information, but also ensuring that the information is collected and maintained in accordance with informed decisions made by the individuals about whom the data pertains.

The following sections discuss some of the harms that may be caused to individuals - due to collection and use of their data – that CNCS must address in the IPP.

E.3.a Invasion of Privacy

Individuals may not want personal information about themselves, such as their religion, sexual orientation, political affiliations, or personal activities, to be revealed to others without their permission. Disclosure of this information could lead to discrimination, personal embarrassment, or damage to one's professional reputation.

Additionally, "Information about a person's financial transactions, including the amount of assets, positions held in stocks or funds, outstanding debts, and purchases can be sensitive. "Information about a person's purchases can reveal a great deal about that person's history, such as places they have visited, whom they have had contact with, products they use, their activities and habits, or medications they have used. In some cases corporations might wish to use this information to target individuals with marketing customized towards those individual's personal preferences, something which that person may or may not approve of."³

Medical records are another area of sensitive information that a person may not want revealed to others. "This may be because they have concern that it might affect their insurance coverage or employment. Or it may be because they would not wish for others to know about medical or psychological conditions or treatment which would be embarrassing. Revealing medical data could also reveal other details about one's personal life (such as about one's sexual activity for example)."⁴

Invasion of Privacy may occur in a variety of ways, including (but not limited to):

- Corporation staff snooping at someone's file out of personal curiosity.
- Accidental posting or exposure of information on the web or other public system.
- Loss of equipment or media containing private information.
- Intentionally hacking into the system or performing dumpster diving to snoop on someone else's information.
- Accessing the system to gain information for blackmail or extortion purposes.
- Intentional exposure of information to cause embarrassment or harm.

³ Wikipedia "Privacy"

⁴ Wikipedia "Privacy"

- Unsecure disposal of paper documents, which either accidentally exposes information or can be exploited by dumpster divers.
- Release or sale of information, without the individual's permission, to businesses that may spam or telemarket the individual.

E.3.b Identity Theft

If criminals gain access to information such as a person's account or credit card numbers that person could become the victim of fraud or identity theft.

“Identity theft—the misuse of another individual’s personal information to commit fraud—can happen in a variety of ways, but the basic elements are the same. Criminals first gather personal information, either through low-tech methods such as stealing mail or workplace records, or “dumpster diving,” or through complex and high-tech frauds such as hacking and the use of malicious computer code. These data thieves then sell the information or use it themselves to open new credit accounts, take over existing accounts, obtain government benefits and services, or even evade law enforcement by using a new identity. Often, individuals learn that they have become victims of identity theft only after being denied credit or employment, or when a debt collector seeks payment for a debt the victim did not incur.”⁵

Identity theft not only causes financial loss, it also affects a person's credit rating which can widespread impact on their lives, from qualification for financial transactions to employment screenings. It also exacts an emotional toll on the individual and their family, who might have to fight for years to get the situation resolved.

Identity theft is a threat from both insiders and outsiders. “According to law enforcement agencies, identity thieves often have no prior criminal background and sometimes have pre-existing relationships with the victims. Indeed, identity thieves have been known to prey on people they know, including coworkers, senior citizens for whom they are serving as caretakers, and even family members... Occasionally, small clusters of individuals with no significant criminal records work together in a loosely knit fashion to obtain personal information and even to create false or fraudulent documents.”⁶

E.3.c Unfair Treatment by the Government

There are additional concerns when information about private citizens is collected by the government. This is particularly an issue when the government uses this data to make decisions, such as awarding benefits or taking criminal action. The Privacy Act was enacted to protect citizens from the Government keeping secret databases of information about them. The Act requires citizens to be notified when their information is collected, informed about its use, and provided access to view and correct the information so that decisions are correctly made. Failing to do so may result in unfair treatment of individuals by the government.

⁵ Identity Theft Task Force, Combating Identity Theft: A Strategic Plan, April 2007

⁶ U.S. Attorney’s Office, Southern District of Florida, Press Release (July 19, 2006), available at <http://www.usdoj.gov/usao/fls/PressReleases/060719-01.html>

F. POLICY FRAMEWORK

Generally speaking, policies are broad statements that summarize management decisions regarding privacy issues. They provide the basic rules for safeguarding sensitive personal and business information. Because policies are very high level, CNCS also needs to develop guidelines and procedures that further define the requirements of the policies and provide guidance on how to implement them.

- *Guidelines* are recommendations that are meant to assist personnel with complying with policy and effectively safeguard sensitive information.
- *Procedures* are specific repeatable instructions for completing a particular process (such as the detailed steps for completing a Privacy Impact Assessment (PIA) or a System of Record Notice (SORN)).
- *Standards* specify the use of particular technologies, procedures, or configurations in particular situations, and are compulsory.

F.1 Relationship to Information Security Program

Information security, as defined under FISMA, encompasses all types of sensitive information, including PII. Thus, information privacy is inextricably linked to information security. Further, in those areas where PII is collected, processed, or stored on an information system, information privacy is a subset of information security.

However, while the protection of PII processed and maintained in information technology systems are largely covered by information security policies and controls governing sensitive information, there are some additional privacy specific requirements that lay outside the information security program boundary. The IPP focuses attention on these requirements while linking to the ISP for shared program components.

Leveraging the linkage between information security and information privacy ensures that compliance with PII protection and handling requirements also results in compliance with the CNCS Information Security Program. Further, the information security guidance regarding techniques for protecting sensitive information (e.g., encryption of sensitive information on mobile devices or when in transit, social engineering countermeasures, and procedures for physically securing media containing sensitive information) will also be applicable to protection of PII. This will reduce the level of effort associated with procedure development and awareness and training while increasing the effectiveness of both the information security and information privacy programs.

F.2 Policy Numbering

Each policy is assigned a unique policy number in the following format:

IPP-XX-YYMM

IPP designates the policy as part of the Information Privacy Program.

XX is a unique number assigned to each policy.

YYMM is the date that the specific version of the policy was issued.

F.3 Policy Structure

The policies are structured to contain the following information:

<i>Policy Name</i>	Formal name of the policy.
<i>Policy Number</i>	Identification number assigned to the policy (see section 6.B).
<i>Subject</i>	Policy statement summarizing the intention of the policy.
<i>Scope</i>	Specification of to whom or what the policy applies.
<i>Description</i>	Explanation of the purpose of the policy.
<i>Procedures, Standards & Guidelines</i>	Narrative stating the specific requirements and directions of the policy. This includes any procedures, standards, and guidelines that must be followed in order to be compliant with the policy.
<i>Roles & Responsibilities</i>	Discussion of responsibilities that apply to each information security role for complying with the policy. Not all roles will have responsibilities for all policies.
<i>Definitions</i>	Defines key terms used in the policy.
<i>Enforcement</i>	Describes the potential penalties for non-compliance with the policy.
<i>Point Of Contact</i>	Specifies the person to contact for additional guidance or questions about the policy.
<i>Attachments</i>	Lists any associated documents that are incorporated into the policy by reference.
<i>Authority</i>	Enumerates the federal laws, regulations, standards, and other authoritative requirements from which the policy is derived.
<i>Effective Date</i>	Specifies the date when the policy goes into effect.
<i>Revision History</i>	Lists any revisions that have been made to the policy document.
<i>Review Schedule</i>	Species the frequency with which the policy should be reviewed for potential revision.

G. INFORMATION PRIVACY ROLES AND RESPONSIBILITIES

Everyone at CNCS has a role in safeguarding sensitive personal and business information. All employees, contractors, and other staff have an obligation to maintain awareness and exercise due diligence in protecting the sensitive information with which they have been entrusted.

However, there are specific information privacy duties that apply to each person depending upon their role within the organization. These roles and responsibilities are described in the following sections.

G.1 General Information Privacy Roles

For the purpose of assigning security and privacy responsibilities, some general roles have been defined. Each policy specifies the particular responsibilities that are assigned to each of these roles as applicable.

Individuals may serve in multiple roles for different aspects of their jobs. For example, a Program Director may serve as an Information Owner for a particular resource, as a Manager for the employees in his/her department, and as a User of information resources.

The roles specified in the CNCS' information security policies are defined as follows.

G.1.a Information Users

Information Users, are individuals who use or have access to CNCS' information resources, including employees, interns, temporary workers, contractors, vendors, and visitors. All individuals who use CNCS information resources are responsible for protecting the resources entrusted to them and complying with CNCS information security policies and procedures.

Information User responsibilities include:

- Adhering to all CNCS information privacy policies.
- Not disclosing any personal information contained in any system of records except as authorized. Personnel willfully making such a disclosure when knowing that disclosure is prohibited are subject to possible criminal penalties and/or administrative sanctions:
and
- Reporting any unauthorized disclosures of personal information from a system of records or the maintenance of any system of records that are not authorized to your local Privacy Act Officer or to your supervisor.

G.1.b Supervisors

Supervisors are employees who have some kind of supervisory relationship over other staff. This can include managers, COTRs, visitor escorts, etc. Supervisors help ensure that their staff

understands their security responsibilities, comply with CNCS policies, and maintain security awareness.

Supervisors are responsible for:

- Ensuring that their staff have the necessary training to effectively comply with CNCS privacy policies and procedures.
- Monitoring staff performance to ensure compliance with CNCS privacy policies.
- Helping to enforce policies.
- Serve as a good example for their employees to follow.
- Providing privacy guidance to their staff.
- Reporting potential violations of privacy policy or potential compromise of PII to the Privacy Officer.
- Implementing remedial actions when their staff violates privacy policies.

G.1.c Information Owners

Information Owners are the individuals ultimately responsible for specific information resources (including data collections). Information Owners are usually managers or directors who own resources on behalf of their departments. It is the information owner's responsibility to ensure that the resources they own are compliant with CNCS information security policies and procedures. Information Owners must be federal staff.

Information Owners are responsible for:

- Identifying PII included in the system for which they are responsible.
- Ensuring that there is authorization and a business need for collection of the identified PII in the system for which they are responsible.
- Including privacy control measures in the Rules of Behavior for their system as appropriate (e.g., encryption of transmission of PII).
- Determining whether the system for which they are responsible constitutes a "System of Records" as defined in the Privacy Act and if so, ensures that a System of Records Notice (SORN) covering their system is in place.
- Reviewing biennially each SORN to ensure that it accurately describes the system of records.
- Making a determination as to whether a PIA is required and submit that determination to the Privacy Officer.
- Ensuring that a PIA is completed on each system as required.
- Ensuring that privacy statements are appropriately posted, comply with CNCS policy, and have been reviewed and approved by the PO and General Counsel.

- Ensuring data collection forms include privacy notification statements.
- Ensuring that systems directed at children incorporate a method for verifiable parent consent for collection of information for children under the age of 13.
- Monitoring contractor compliance with the Privacy Act.
- Ensuring users of the system are trained on the specific handling requirements and safeguards.
- Ensuring that a log is maintained of access and amendments to records, and disclosures of the records.
- Ensuring that CNCS websites do not employ persistent tracking technologies.
- Implementing, testing, and maintaining machine-readable privacy policies on existing websites and websites in development.
- Ensuring that a privacy policy has been developed and is accessible as a link on each CNCS webpage.
- Ensuring that the systems and programs for which they are responsible include appropriate requirements for the identification and protection of PII in accordance with CNCS policy.
- Ensuring that the use of PII is restricted to the minimum necessary to complete program objectives.
- Ensuring that official files on individuals that are retrieved by name or other personal identifier are not maintained without first ensuring that a Privacy Act system of records notice has been published in the Federal Register. Any official, who willfully maintains a system of records without meeting the publication requirements of the Act, is subject to possible criminal penalties and/or administrative sanctions.
- Reporting potential violations of privacy policy or potential compromise of PII to the Privacy Officer.

G.1.d Information Custodians

Information Custodians are individuals who maintain or administer information resources on behalf of Information Owners. All individuals who design, develop, maintain, or administer a CNCS information system or the data it contains are responsible for protecting the CNCS resources under their control and complying with CNCS information security policies and procedures. These individuals can be CNCS employees, contractors, or other kinds of staff.

G.2 Designated Roles

In addition to the general roles described above, there are individuals at CNCS who have been assigned additional responsibilities regarding the safeguarding of sensitive personal information. A list of current assignees at the time of policy issuance is included in Appendix C.

G.2.a Chief Executive Officer (CEO)

The Chief Executive Officer (CEO) of CNCS is responsible for ensuring that the information privacy policies, procedures, and practices of the Corporation are adequate.

The CEO is responsible for:

- Ensuring compliance with statutory and regulatory privacy requirements.
- Designating a Senior Agency Official for Privacy (SAOP) who has the overall agency-wide responsibility for information privacy issues.
- Ensuring that the CIO, in coordination with the other agency officials, reports annually on the effectiveness of the agency information privacy program, including the progress of remedial actions.
- Ensuring that information privacy is integrated into strategic and operational planning processes.
- Ensuring that senior agency officials within the organization are given the necessary authority and resources to effectively implement and manage the privacy policies.

G.2.b Senior Agency Official For Privacy

The Senior Agency Official for Privacy has overall responsibility and accountability for ensuring the agency's implementation of information privacy protections, including the agency's full compliance with federal laws, regulations, and policies relating to information privacy.

The Senior Agency Official for Privacy has the following privacy responsibilities:

- Designating a Privacy Officer responsible for developing, implementing, and maintaining an information privacy program.
- Overseeing, coordinating and facilitating agency compliance with statutory and regulatory privacy requirements.
- Reporting annually, in coordination with the other senior agency officials, to the agency head on the effectiveness of the agency information privacy program, including the progress of remedial actions.

G.2.c Privacy Officer

The Privacy Officer is responsible for developing and operating the Privacy program, and ensuring privacy compliance across the organization. The Privacy Officer is responsible for:

- Maintaining awareness of privacy laws, regulations, and issues within the CNCS.
- Reviewing and implementing privacy regulations and legislation.
- Developing privacy policies and guidance and ensuring their dissemination and implementation throughout the Corporation.

- Establishing a process to inform and educate employees and contractors of their responsibility for protecting PII.
- Coordinating privacy reporting activities as mandated by federal privacy legislation and OMB guidance.
- Reviewing annually each ongoing matching program in which the agency has participated during the year.
- Ensuring that PIAs and SORNs are properly posted.
- Coordinating with the Privacy Act Officer and Privacy Advocate to ensure agency privacy statements, reports, contracts, and notices are compliant with the E-Government Act, privacy guidelines, and agency policy.
- Preparing guidelines for the use of PII and associated privacy protections to be applied to CNCS websites and systems.
- Maintaining a Plan of Actions and Milestones (POA&M) that monitors and tracks the completion of activities intended to mitigate privacy program control weaknesses affecting PII.
- Supporting the Senior Agency Official for Privacy in annual reporting to the agency head on the effectiveness of the agency privacy program.

G.2.d Privacy Act Officer

The Office of the General Counsel (OGC) is responsible for review of all legal documents for the Corporation. OGC assigns one of their staff to serve as the Freedom of Information Act (FOIA) Officer and the Privacy Act Officer to adjudicate records requests.

The Privacy Act Officer is responsible for:

- Reviewing CNCS Privacy Act System of Records Notices (SORN) prior to publication.
- Responding to and reviewing Privacy Act related questions in the Agency Privacy Management Report section of FISMA.
- Reviewing privacy statements, reports, contracts, and notices to ensure compliancy with the E-Government Act, privacy guidelines, and agency policy.
- Advising the CEO and the Senior Agency Official for Privacy on matters involving interpretation of the provisions of the Privacy Act.
- Reviewing biennially the actions of CNCS personnel that have resulted either in CNCS being found civilly liable under Section (g) of the Privacy Act or an employee being found criminally liable under the provisions of Section (i) of the Privacy Act, in order to determine the extent of the problem, and to find the most effective way to prevent recurrence of the problem.
- Responding to Freedom of Information Act (FOIA) requests.

- Supporting the Senior Agency Official for Privacy in annual reporting to the agency head on the effectiveness of the agency privacy program.

G.2.e Chief Information Security Officer (CISO)

The CISO ensures the confidentiality, integrity and availability of information and information systems through formal policies, awareness training, monitoring compliance and access controls. The CISO identifies and assesses risk, explores controls and countermeasures, provides recommendations to senior management, develops and obtains senior management approval of policies and procedures, and implements approved policies and procedures.

The CISO has the following responsibilities related to information privacy:

- Integrating and implementing security policies, procedures, and practices that are consistent with CNCS Privacy requirements to ensure that systems, programs, and PII are secure.
- Developing and maintaining risk-based information security policies, procedures, and control techniques to address all applicable requirements throughout the life cycle of each agency information system to ensure compliance with applicable requirements.
- Ensuring that agency personnel, including contractors, receive appropriate training on protecting information.
- Periodically testing and evaluating the effectiveness of information security policies, procedures, and practices that protect privacy information.
- Establishing and maintaining a process for planning, implementing, evaluating, and documenting remedial action to address any deficiencies in the information security policies, procedures, and practices of the agency.
- Developing and implementing procedures for detecting, reporting, and responding to incidents.
- Periodically assessing risk and magnitude of the harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of privacy information.

G.2.f Chief Information Officer (CIO)

The Chief Information Officer (CIO) oversees the programs of the Office of Information Technology. The CIO plans the nature and extent of IT operations and activities for CNCS, and ensures that IT management directly supports CNCS' strategic mission. The CIO promotes a coordinated, interoperable, secure and shared corporate IT infrastructure. Additionally, the CIO serves as a corporate-wide resource for major policy, program, or operational initiatives, and provides advice on technical information technology issues that may impact the creation and maintenance of cooperative agreements with customers and stakeholders. Per the Federal Information Security Management Act (FISMA) and OMB implementing directives, the CIO monitors, evaluates and reports the status of information security and privacy within the Agency to the Chief Executive Officer (CEO) of CNCS.

The Chief Information Officer is responsible for:

- Developing and maintaining IT procedures and control techniques to address privacy requirements.
- Working to ensure that IT systems and practices are compliant with applicable information privacy requirements.
- Participating in and supporting incident response activities.
- Reporting annually, in coordination with the other senior agency officials, to the agency head on the effectiveness of the agency information privacy program, including progress of remedial actions.

G.2.g Chief Human Capital Officer (CHCO)

The Chief Human Capital Officer (CHCO) is responsible for the security and privacy of the Corporation's personnel records. The CHCO assigns one of his staff to serve as the Privacy Advocate.

The CHCO is responsible for:

- Establishing procedures for proper handling and protection of personnel records.
- Designating a Privacy Advocate to address personnel privacy issues.
- Requiring all employees responsible for the creation, development, maintenance, processing, use, dissemination, and safeguarding of personnel records to be familiar with the rules of conduct presented in this section.
- Ensuring that administrative, technical, physical, and security safeguards for personnel data in automated records have been established.
- Limiting the collection and use of employee social security numbers and personal information to the minimum required.
- Ensuring that personnel information is only disclosed as permitted under established regulations.
- In concert with the Privacy Officer, review biennially agency recordkeeping and disposal policies and practices in order to assure compliance with the Privacy Act.
- Supporting the Senior Agency Official for Privacy in annual reporting to the agency head on the effectiveness of the agency privacy program.

G.2.h Privacy Advocate

The Privacy Advocate ensures that privacy is considered within the Office of Human Capital (OHC) programs and business processes. The Privacy Advocate reviews and evaluates activities related to personally identifiable information collected and maintained by the Office of Human Capital (OHC).

The Privacy Advocate is responsible for:

- Identifying and reporting all OHC systems or projects that collect personally identifiable information.
- Ensuring that appropriate physical, technical, and administrative safeguards are implemented for the security and accuracy of OHC records to prevent substantial harm, embarrassment, inconvenience, or unfairness to any individual on whom information is maintained.
- Establishing procedures for ensuring that individuals responsible for processing and maintaining privacy paper records conduct an end of day security check of their work area, including securing away any sensitive documents they have at their desk.
- Ensuring that the unnecessary printing and displaying of the SSN or forms, reports, and computer display screens is eliminated.
- If Social Security Numbers are collected, ensuring they are collected at the time of an employee's appointment and entered into the human resources and payroll systems. The collection tool (if paper-based) should be stored in a secure location until it is no longer required.
- Ensuring that access to the SSN is restricted to only those individuals whose official duty requires such access.
- Ensuring that a listing of all access authorization is maintained and monitored regularly for continued applicability.
- Ensuring that Human Capital policies and written agreements are in compliance with Federal privacy protection policies, including policies governing the protection of employee Social Security Numbers.
- Ensuring that paper-based records containing PII is transported properly.
- Ensuring that access to employee PII, including data entry, printing, and screen displays are conducted in a secure location to protect against unauthorized exposures.
- Ensuring that all security incidents involving employee PII are reported in a timely manner in accordance with CNCS Information Security Policy.
- Ensuring that written procedures describing the proper labeling, storage, and disposal of printed material containing employee PII is established and communicated to employees.
- Ensuring that all disclosures of employee PII are made in accordance with established regulations and procedures.
- Ensure internal control procedures are employed to ensure the proper monitoring of authorized and unauthorized access to Social Security Numbers and other personally identifiable information.
- Regularly reviewing procedures, at least annually, to ensure they are effective and update as necessary.

G.2.i Inspector General (IG)

Office of the Inspector General (OIG) investigates, audits, and takes other action in accordance with the Inspector General Act to detect, prevent, and investigate wrongdoing. In accordance with FISMA, the OIG conducts an annual independent assessment of the CNCS information privacy program to assess the Corporation's privacy practices and identify additional measures needed.

The IG is responsible for:

- Identifying operational deficiencies within the organization.
- Ensuring that the underlying problems that permit such failings are rectified.
- Offering recommendations for preventing problems in the future.
- Conducting an annual independent assessment of CNCS' information security and privacy programs.
- Reviewing CNCS' FISMA and agency Privacy Management submission to OMB.

G.2.j Procurement Services

The Acquisitions/Contracting function is responsible for managing contracts and overseeing their implementation.

Contracting Officers are responsible for:

- In concert with the Privacy Officer, review every two years a random sample of agency contracts that provide for the maintenance of a system of records on behalf of the agency to accomplish an agency function, in order to ensure that the wording of each contract makes the provisions on the contractor and his or her employees.
- Ensuring that CNCS solicitation documents and contracts include appropriate security and privacy language.
- Reviewing and adjudicating reported incidents where contractor personnel appear to have violated CNCS Privacy Policy and Procedures or otherwise compromised PII. In such instances, the Contracting Officer shall impose the sanctions provided in the appropriate contract or forward the incident for criminal prosecution.
- Supporting the Senior Agency Official for Privacy in annual reporting to the agency head on the effectiveness of the agency privacy program.

G.2.k Contracting Officer's Technical Representative (COTR)

Contracting Officer's Technical Representatives are qualified individuals appointed by the Contracting Officer to assist in the technical monitoring or administration of a contract.

COTRs are responsible for:

- Ensuring that contractor staff assigned to contracts for which they are responsible have appropriate background screening in accordance with contract requirements.
- Monitoring contract activities to minimize the potential for a compromise of PII and to ensure compliance with security and privacy requirements in the contract.
- Reporting or forwarding reports of potential compromise of PII to the Contracting Officer for adjudication and possible sanctions.
- Ensuring that official files on individuals that are retrieved by name or other personal identifier are not maintained without first ensuring that a Privacy Act system of records notice has been published in the Federal Register. Any official, who willfully maintains a system of records without meeting the publication requirements of the Act, is subject to possible criminal penalties and/or administrative sanctions.
- Monitoring contractor activities to ensure that contractor staff have appropriate instruction and training regarding the requirements for protecting PII.

G.2.1 Grants Program Officer

Privacy must also be addressed by grantees and others involved in the award and management of grants. The Grants Program Officer is responsible for ensuring that CNCS privacy policies are followed throughout the grant lifecycle and for coordinating with grantees for compliance and privacy issues.

H. POLICIES

Based on the analysis of the information privacy requirements presented in section E, CNCS has developed a set of policies to meet its privacy needs. These have been developed in accordance with the framework specified in section F. Additional policies will be defined as needs arise. The policies currently include:

Policy #	Policy Name	Summary
IPP-01	Privacy Governance & Reporting	CNCS will manage and report on the status of its information privacy program as required by FISMA and OMB.
IPP-02	Privacy Training & Awareness	CNCS will implement a program to maintain awareness of information privacy policies, standards and acceptable practices.
IPP-03	Rules and Consequences	All staff at CNCS have a duty to protect personally identifiable information (PII) from loss or misuse.
IPP-04	Privacy Incident Management	The Corporation must be able to respond to privacy-related incidents in a manner that protects its own information and helps to protect the information of others that might be affected by the incident.
IPP-05	Collecting & Protecting Personally Identifiable Information	CNCS will implement appropriate safeguards and procedures when collecting, storing, and handling personal information in order to protect individuals' privacy rights.
IPP-06	Privacy Impact Assessments (PIA)	CNCS must conduct privacy impact assessments before developing, procuring, or substantially modifying information technology (IT) projects or systems that collect, maintain, or disseminate information in identifiable form and make them publicly available.
IPP-07	Systems of Records	CNCS will publish notices for its systems of records in accordance with Privacy Act requirements, and will periodically review them to ensure that they are accurate and complete.
IPP-08	Web Site Privacy	CNCS must protect an individual's right to privacy when personal information is collected on Corporation web sites.
IPP-09	Computer Data Matching	Special procedures are required when conducting computer matching programs.
IPP-10	Data Extracts	All computer-readable data extracts from databases holding sensitive information must be logged and verified.

APPENDIX A: FEDERAL REQUIREMENTS AND GUIDANCE

H.1 The Privacy Act of 1974 (5 U.S.C. § 552a) as amended, PL 93-579, December 31, 1974

The Privacy Act of 1974 is the primary act that regulates the federal government's use of personal information. The Privacy Act places limitations on agencies' collection, disclosure, and use of personal information in systems of records. A system of records is a collection of information about individuals under the control of an agency from which information is actually retrieved by the name of the individual or by some identifying number, symbol, or other particular assigned to the individual. The act does not apply when there is merely a capability or potential for retrieval by identifier. Among the major provisions of the Privacy Act are the following:

- **Collecting only necessary information.** Agencies are to maintain personal information about an individual only when it is relevant and necessary to accomplish a purpose of the agency required to be accomplished by statute or executive order of the President. According to OMB guidance, the goal of this provision is to reduce the amount of personal information that agencies collect in order to reduce the risk of agencies' improperly using personal information.
- **Providing public notice.** Agencies are to publish a notice in the Federal Register when establishing or revising a system of records. The notice is to contain the name and location of the system, the categories of individuals on whom records are maintained in the system, and each "routine use" of the records contained in the system.
- **Providing for informed consent.** Agencies are to inform individuals whom it asks to supply information of (1) the authority for soliciting the information and whether disclosure of such information is mandatory or voluntary, (2) the principal purposes for which the information is intended to be used, (3) the routine uses that may be made of the information, and (4) the effects on the individual, if any, of not providing the information.

The Act requires agencies to establish rules of conduct for persons involved in the design, development, operation, or maintenance of any system of records, or in maintaining any record, and to instruct each person on the rules and the requirements of the Privacy Act.

H.2 The Computer Matching and Privacy Protection Act of 1988 (5 U.S.C. § 552a note)

The Computer Matching and Privacy Protection Act of 1988 amended the Privacy Act by establishing the conditions under which computer matching involving the Federal government could be performed and adding certain protections for individuals applying for and receiving Federal benefits. Section 7201 of the Omnibus Budget Reconciliation Act of 1990 (Pub. L. 101-508) further amended the Privacy Act regarding protections for such individuals.

The Privacy Act, as amended, regulates the use of computer matching by Federal agencies when records in a system of records are matched with other Federal, State, or local government

records. Among other things, it requires Federal agencies involved in computer matching programs to:

- Negotiate written agreements with the other agency or agencies participating in the matching programs.
- Obtain the approval of the match agreement by the Data Integrity Branch (DIB) of the participating Federal agencies.
- Furnish detailed reports about matching programs to Congress and OMB.
- Notify applicants and beneficiaries that their records are subject to matching.
- Verify match findings before reducing suspending, terminating or denying an individual's benefits or payments.

H.3 Computer Matching and Privacy Protection Amendments of 1990, PL 101-508.

Congress enacted the Computer Matching and Privacy Protection Amendments of 1990 (Pub. L. No. 101-508), to further clarify the due process provisions found in subsection (p).

H.4 The Government Paperwork Reduction Act of 1995 (44 U.S.C. § 101 note) and the Information Technology Management Reform Act of 1996 (also known as Clinger-Cohen Act; 41 U.S.C. § 251)

The Paperwork Reduction Act and the Information Technology Management Reform Act linked agency privacy activities to information technology and information resources management. Both assign the responsibility to ensure implementation of privacy within their agencies to the Chief Information Officer (CIO) .

H.5 OMB Circular A-130, Transmittal No. 3, Appendix I, "Federal Agency Responsibilities for Maintaining Records About Individuals," February 8, 1996.

In 1996, OMB issued Circular A-130, Appendix I specifying content of and procedures for providing required public notices and describing agency obligations to report to OMB on privacy activities and compliance with the Act.

H.6 OMB Circular A-123, "Management Accountability and Controls," June 21, 1995.

Issued under Federal Managers' Financial Integrity Act of 1982 as codified in 31 U.S.C. 3512. Requires internal controls to prevent fraud, waste, and abuse. Primarily applies to financial systems.

H.7 The Health Insurance Portability and Accountability Act (HIPAA) of 1996, Public Law 104-191, August 21, 1996

The HIPAA Security Rule specifically focuses on the safeguarding of electronic protected health information (EPHI). Although FISMA applies to all federal agencies and all information types, only a subset of agencies is subject to the HIPAA Security Rule based on their functions and use of EPHI. All HIPAA covered entities, which includes some federal agencies, must comply with the Security Rule. The Security Rule specifically focuses on protecting the confidentiality, integrity, and availability of EPHI, as defined in the Security Rule. The EPHI that a covered entity creates, receives, maintains, or transmits must be protected against reasonably anticipated threats, hazards, and impermissible uses and/or disclosures. In general, the requirements, standards, and implementation specifications of the Security Rule apply to the following covered entities:

- Covered Health Care Providers. Any provider of medical or other health services, or supplies, who transmits any health information in electronic form in connection with a transaction for which the Department of Health and Human Services (HHS) has adopted a standard.
- Health Plans. Any individual or group plan that provides or pays the cost of medical care (e.g., a health insurance issuer and the Medicare and Medicaid programs).
- Health Care Clearinghouse. A public or private entity that processes another entity's health care transactions from a standard format to a non-standard format, or vice-versa.
- Medicare Prescription Drug Card Sponsors. A nongovernmental entity that offers an endorsed discount drug program under the Medicare Modernization Act. This fourth category of "covered entity" will remain in effect until the drug card program ends in 2006.

HIPAA indirectly covers "business associates" and any other entity that uses or discloses personal health information whether or not such an entity falls under the definition of health care provider, health plan or health care clearinghouse.

H.8 Freedom of Information Act (FOIA)

The Freedom of Information Act (FOIA), 5 U.S.C. § 552, was enacted in 1966 and generally provides that:

- Any person has the right to request access to federal agency records or information.
- All agencies of the U.S. Government are required to disclose records upon receiving a written request for them.
- There are nine exemptions to the FOIA that protect certain records from disclosure.

H.9 Section 208 of the E-Government Act of 2002 (44 U.S.C. § 3501 note) Pub. L. No. 107-347, Dec. 17, 2002

The E-Government Act of 2002 strives to enhance protection for personal information in government information systems or information collections by requiring that agencies conduct privacy impact assessments (PIA). A PIA is an analysis of how personal information is collected, stored, shared, and managed in a federal system. More specifically, according to OMB guidance, a PIA is an analysis of how information is handled.

Specifically, a PIA is conducted to:

- Ensure that handling conforms 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.
- Examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks.

Agencies must conduct PIAs before developing or procuring information technology that collects, maintains, or disseminates information that is in a personally identifiable form; or before initiating any new data collections involving personal information that will be collected, maintained, or disseminated using information technology if the same questions are asked of 10 or more people. To the extent that PIAs are made publicly available, they provide explanations to the public about such things as the information that will be collected, why it is being collected, how it is to be used, and how the system and data will be maintained and protected.

H.10 Federal Information Security Management Act of 2002 (FISMA), PL 107-347, December 17, 2002

FISMA also addresses the protection of personal information. FISMA defines federal requirements for securing information and information systems that support federal agency operations and assets; it requires agencies to develop agency wide information security programs that extend to contractors and other providers of federal data and systems. Under FISMA, information security means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction, including controls necessary to preserve authorized restrictions on access and disclosure to protect personal privacy, among other things. As part of annual reporting under FISMA, agencies report on how they are implementing the requirements of privacy laws and policy in the areas of privacy leadership and coordination, procedures and practices, and internal oversight.

H.11 Office of Management and Budget (OMB) Memoranda

OMB issues memoranda that provide instructions to agency officials regarding various issues. Some memoranda that apply to information privacy include:

- M-07-19, FY 2007 Reporting Instructions for the Federal Information Security

Management Act and Agency Privacy Management (July 25, 2007)

- M-07-16 Data Extract Frequently Asked Questions
- M-07-16, Safeguarding Against and Responding to the Breach of Personally Identifiable Information (May 22, 2007))
- M-07-04, Use of Commercial Credit Monitoring Services Blanket Purchase Agreements (BPA) (December 22, 2006)
- Recommendations for Identity Theft Related Data Breach Notification (September 20, 2006)
- M-06-19, Reporting Incidents Involving Personally Identifiable Information Incorporating the Cost for Security in Agency Information Technology Investments (July 12, 2006)
- M-06-16, Protection of Sensitive Agency Information (June 23, 2006)
- M-06-15, Safeguarding Personally Identifiable Information (May 22, 2006)
- M-05-08, Designation of Senior Agency Officials for Privacy (February 11, 2005)
- M-03-22, OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002 (September 30, 2003)
- M-01-05, Guidance on Inter-Agency Sharing of Personal Data - Protecting Personal Privacy (December 20, 2000)
- M-00-13, Privacy Policies and Data Collection on Federal Web Sites (June 22, 2000)
- M-99-18, Privacy Policies on Federal Web Sites (June 2, 1999)
- M-99-05, Instructions on Complying with President's Memorandum of May 14, 1998, "Privacy and Personal Information in Federal Records" (January 7, 1999)
- Privacy Act Implementation, Guidelines and Responsibilities, 40 FR 28948 (July 9, 1975).

H.12 National Institute of Standards & Technology (NIST) Guidance

Founded in 1901, NIST is a non-regulatory federal agency within the U.S. Commerce Department's Technology Administration. NIST's mission is to develop and promote measurement, standards, and technology to enhance productivity, facilitate trade, and improve the quality of life. Some NIST publications that apply to information privacy include:

- Federal Information Processing Standards Publication (FIPS) 199, Standard for Security Categorization of Federal Information and Information Systems, February 2004.
- NIST Special Publication 800-53, Recommended Security Controls for Federal Information Systems, February 2005.
- NIST Special Publication 800-53A, Guide for Assessing the Security Controls in Federal Information Systems (Second Public Draft), April 2006.

- NIST Special Publication 800-66, An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule, March 2005.
- NIST Special Publication 800-92, Guide to Computer Security Log Management.

H.13 5 CFR part 293, “Personnel Records,” January 1, 2001

This sets forth basic policies governing the creation, development, maintenance, processing, use, dissemination, and safeguarding of personnel records which the Office of Personnel Management requires agencies to maintain in the personnel management or personnel policy setting process.

H.14 Executive Order 13402, May 10, 2006, President’s Identity Theft Task Force and the Task Force’s report: Combating Identity Theft – A Strategic Plan, April 2007

The President established the Task Force to define the issues and challenges posed by identity theft and develop a strategic response plan. This document reports on its findings.

H.15 GAO-08-343 Protecting Personally Identifiable information (January 2008)

"The loss of personally identifiable information can result in substantial harm, embarrassment, and inconvenience to individuals and may lead to identity theft or other fraudulent use of the information. As shown in prior GAO reports, compromises to such information and long-standing weaknesses in federal information security raise important questions about what steps federal agencies should take to prevent them. As the federal government obtains and processes information about individuals in increasingly diverse ways, properly protecting this information and respecting the privacy rights of individuals will remain critically important.

GAO was requested to (1) identify the federal laws and guidance issued to protect personally identifiable information from unauthorized use or disclosure and (2) describe agencies’ progress in developing policies and documented procedures that respond to recent guidance from the Office of Management and Budget (OMB) to protect personally identifiable information that is either accessed remotely or physically transported outside an agency’s secured physical perimeter. To do so, GAO reviewed relevant laws and guidance, surveyed officials at 24 major federal agencies, and examined and analyzed agency documents, including policies, procedures, and plans. In commenting on a draft of this report, OMB stated that it generally agreed with the report’s contents. "

H.16 Gramm-Leach-Bliley Act (GLBA)

Requires financial institutions to provide each consumer with a privacy notice at the time the consumer relationship is established and annually thereafter. The privacy notice must explain the information collected about the consumer, where that information is shared, how that information is used, and how that information is protected. The notice must also identify the

consumer's right to opt-out of the information being shared with unaffiliated parties per the Fair Credit Reporting Act. Should the privacy policy change at any point in time, the consumer must be notified again for acceptance. Each time the privacy notice is reestablished, the consumer has the right to opt-out again. The unaffiliated parties receiving the nonpublic information are held to the acceptance terms of the consumer under the original relationship agreement.

GLBA also requires financial institutions to develop a written information security plan that describes how the company is prepared for, and plans to continue to protect clients' nonpublic personal information. This plan must include:

- Denoting at least one employee to manage the safeguards,
- Constructing a thorough [risk management] on each department handling the nonpublic information,
- Develop, monitor, and test a program to secure the information, and
- Change the safeguards as needed with the changes in how information is collected, stored, and used.

The GLBA defines "financial institutions" as: "...companies that offer financial products or services to individuals, like loans, financial or investment advice, or insurance. The Federal Trade Commission (FTC) has jurisdiction over financial institutions similar to, and including, non-bank mortgage lenders, loan brokers, some financial or investment advisers, debt collectors, tax return preparers, banks, and real estate settlement service providers. These companies must also be considered significantly engaged in the financial service or production that defines them as a "financial institution".

H.17 Fair Credit Reporting Act (FCRA)

FCRA regulates the collection, dissemination, and use of consumer credit information.

Consumer reporting agencies (CRAs), entities that collect and disseminate information about consumers to be used for credit evaluation and certain other purposes, must:

- Provide a consumer with information about him or her in the agency's files and to take steps to verify the accuracy of information disputed by a consumer. Under the Fair and Accurate Credit Transactions Act (FACTA), an amendment to the FCRA passed in 2003, consumers are able to receive one free credit report a year. The free report can be requested by telephone, mail, or through the government-authorized website, annualcreditreport.com.
- If negative information is removed as a result of a consumer's dispute, it may not be reinserted without notifying the consumer within five days, in writing.
- CRAs may not retain negative information for an excessive period. The FCRA spells out how long negative information, such as late payments, bankruptcies, tax liens or judgments may stay on a consumer's credit report — typically seven years from the date of the delinquency. The exceptions: bankruptcies (10 years) and tax liens (seven years from the time they are paid).

Under the FCRA, information furnishers (a company that provides information to consumer reporting agencies) may only report to a consumer's credit report under the following guidelines:

- They must provide complete and accurate information to the credit rating agencies.
- The duty to investigate disputed information from consumers falls on them.
- They must inform consumers about negative information which has been or is about to be placed on a consumer's credit report within 30 days (they must correct the error or explain why the credit report is correct within 90 days).

Users of the information for credit, insurance, or employment purposes (including background checks) have the following responsibilities under the FCRA:

- They must notify the consumer when an adverse action is taken on the basis of such reports.
- Users must identify the company that provided the report, so that the accuracy and completeness of the report may be verified or contested by the consumer.

H.18 Children's Online Privacy Protection Act (COPPA)

The Children's Online Privacy Protection Act, effective April 21, 2000, applies to the online collection of personal information from children under 13. The new rules spell out what a Web site operator must include in a privacy policy, when and how to seek verifiable consent from a parent and what responsibilities an operator has to protect children's privacy and safety online.

If you operate a commercial Web site or an online service directed to children under 13 that collects personal information from children or if you operate a general audience Web site and have actual knowledge that you are collecting personal information from children, you must comply with the Children's Online Privacy Protection Act.

The Children's Online Privacy Protection Act and Rule apply to individually identifiable information about a child that is collected online, such as full name, home address, email address, telephone number or any other information that would allow someone to identify or contact the child. The Act and Rule also cover other types of information -- for example, hobbies, interests and information collected through cookies or other types of tracking mechanisms -- when they are tied to individually identifiable information.

An operator must post a link to a notice of its information practices on the home page of its Web site or online service and at each area where it collects personal information from children. An operator of a general audience site with a separate children's area must post a link to its notice on the home page of the children's area. The link to the privacy notice must be clear and prominent. Operators may want to use a larger font size or a different color type on a contrasting background to make it stand out. A link in small print at the bottom of the page -- or a link that is indistinguishable from other links on your site -- is not considered clear and prominent.

APPENDIX B: ACRONYMS AND ABBREVIATIONS

<i>BII</i>	Business Identifiable Information	<i>OGC</i>	Office of the General Counsel
<i>CEO</i>	Chief Executive Officer	<i>OIG</i>	Office of the Inspector General
<i>CFR</i>	Code of Federal Regulations	<i>OIT</i>	Office of Information Technology
<i>CHCO</i>	Chief Human Capital Officer	<i>OHC</i>	Office of Human Capital
<i>CIO</i>	Chief Information Officer	<i>OMB</i>	Office of Management and Budget
<i>CISO</i>	Chief Information Security Officer	<i>PAO</i>	Privacy Act Officer
<i>CNCS</i>	Corporation for National & Community Service	<i>PL</i>	Public Law
<i>COTR</i>	Contracting Officer's Technical Representative	<i>PIA</i>	Privacy Impact Assessment
<i>FISMA</i>	Federal Information Security Management Act	<i>PII</i>	Personally Identifiable Information
<i>FOIA</i>	Freedom of Information Act	<i>PO</i>	Privacy Officer
<i>HIPAA</i>	Health Insurance Portability and Accountability Act	<i>POA&M</i>	Plan of Action and Milestones
<i>IIF</i>	Information in Identifiable Form	<i>ROB</i>	Rules of Behavior
<i>IPP</i>	Information Privacy Program	<i>SAOP</i>	Senior Agency Official for Privacy
<i>ISP</i>	Information Security Program	<i>SETA</i>	Security Education, Training & Awareness
<i>IT</i>	Information Technology	<i>SORN</i>	System of Records Notice
<i>NARA</i>	National Archives and Records Administration	<i>SSN</i>	Social Security Number
<i>NIST</i>	National Institute of Standards & Technology	<i>USC</i>	United States Code

APPENDIX C: INFORMATION PRIVACY ROLE ASSIGNMENTS (AS OF APRIL 2008)

Role	Individual Assigned
Chief Executive Officer (CEO)	David Eisner
Chief Information Officer (CIO)	R. Alan Friend (Acting)
Chief Information Security Officer (CISO)	Juliette Sheppard
Privacy Officer	Laurie Young
Senior Agency Official for Privacy (SAOP)	R. Alan Friend (Acting)
Privacy Act Officer	Austin Holland
Privacy Advocate	Norm Franklin
Chief Human Capital Officer (CHCO)	Ray Limon
Inspector General	Gerald Walpin
Director of Procurement Services	Roderick Gaither

APPENDIX D: INFORMATION PRIVACY POLICY DOCUMENTS

PRIVACY PROGRAM GOVERNANCE AND REPORTING

IPP-01-0808

1. **SUBJECT:** Information Privacy must be managed and governed to reduce risks to CNCS operations and to individuals' private information. CNCS will manage its Information Privacy program to proactively track and mitigate weaknesses, and will report on the status of the program as required by OMB.
2. **SCOPE:** This policy applies to management and reporting of the CNCS information Privacy program.
3. **DESCRIPTION:** CNCS collects personal information about individuals for a variety of authorized purposes. CNCS must protect these individuals' rights to privacy by guarding against unauthorized disclosure or misuse of their personal information.

As a Federal Corporation, CNCS is required by the Privacy Act and other legislation to implement practices to protect personal information. CNCS must conduct reviews to verify compliance with privacy requirements, and promptly identify deficiencies and risks. The Corporation is also obligated to take appropriate steps to remedy any deficiencies found. Agencies are also required to maintain appropriate documentation regarding their compliance with information privacy laws, regulations, and policies.

4. PROCEDURES & GUIDELINES:

- (a) CNCS will operate an Information Privacy Program (IPP) in compliance with the Privacy Act, Section 208 of the E-Government Act of 2002, and other federal laws and guidance.
- (b) The IPP complements the Information Security Program which provides for protection of all of the Corporation's information. Privacy policies and practices will ensure that information is handled in a manner that maximizes both privacy and security.
- (c) The CEO will designate a Senior Agency Official for Privacy (SAOP) who assumes overall responsibility and accountability for ensuring the agency's implementation of information privacy protections, including the Corporation's full compliance with federal laws, regulations, and policies relating to information privacy, such as the Privacy Act.
- (d) The IPP will be continuously assessed and updated to ensure that privacy data is adequately protected, federal requirements are being met, and the program is operating as intended.

- (1) The Corporation will conduct a periodic review (on at least an annual basis) of its policies and processes, and take corrective action as appropriate to ensure that CNCS has adequate safeguards to prevent the intentional or negligent misuse of, or unauthorized access to, personally identifiable information (PII). This review shall address all administrative, technical, and physical means used by the Corporation to control such information.
- (2) On at least a monthly basis, the Privacy Officer will check OMB, NIST, and other sources for any new Privacy-related guidance or requirements.
 - For any new privacy law or OMB/NIST privacy guidance that is issued, CNCS will develop a plan and schedule for ensuring compliance with the new requirement(s).
- (e) CNCS will maintain a Plan of Actions & Milestones (POA&M) to track identified privacy program deficiencies and remedial actions planned and implemented for those deficiencies.
 - (1) The Privacy POA&M will be integrated with the Information Security POA&Ms and will address Privacy-specific issues not covered under the ISP and System-level POA&Ms.
 - (2) The Privacy Officer will develop and maintain the Privacy POA&M and provide updates to the CISO on a periodic basis for inclusion in FISMA reporting.
 - (3) Any official reports providing specific information on Privacy weaknesses resulting from Inspector General audits, internal reviews, or privacy incidents will be documented as part of the POA&M.
 - (4) The POA&M will be continuously updated as items are completed and new weaknesses discovered so that it reflects the current state of the Corporation's mitigation status.
- (f) OMB requires annual reports on the Corporations information privacy status under FISMA and the President's Management Agenda Scorecard. Reports will be completed and submitted in accordance with the latest OMB guidance. Additionally, CNCS will provide other applicable privacy-related reports when requested by OMB.
- (g) CNCS will conduct Privacy Act mandated reviews and will be prepared to report to the Director of OMB on the results of those reviews.
 - (1) Section M Contracts - Review every two years a random sample of Corporation contracts that provide for the maintenance of a system of records on behalf of the Corporation to accomplish a Corporation function, in order to ensure that the wording of each contract makes the provisions of the Act binding on the contractor and his or her employees. (See 5 U.S.C. 552a(m)(1))
 - (2) Records Practices - Review biennially Corporation recordkeeping and disposal policies and practices in order to assure compliance with the Act, paying particular attention to the maintenance of automated records.

- (3) Routine Uses - Review every four years the routine use disclosures associated with each system of records in order to ensure that the recipient's use of such records continues to be compatible with the purpose for which the disclosing Corporation collected the information.
- (4) Exemptions - Review every four years each system of records for which the Corporation has promulgated exemption rules pursuant to Section (j) or (k) of the Act in order to determine whether such exemption is still needed.
- (5) Matching Programs – Review annually each ongoing matching program in which the Corporation has participated during the year in order to ensure that the requirements of the Act, the OMB guidance, and any Corporation regulations, operating instructions, or guidelines have been met.
- (6) Training - Review biennially Corporation training practices in order to ensure that all Corporation personnel are familiar with the requirements of the Act, with CNCS' implementing regulation, and with any special requirements of their specific jobs.
- (7) Violations - Review biennially the actions of Corporation personnel that have resulted either in the Corporation being found civilly liable under Section (g) of the Act, or an employee being found criminally liable under the provisions of Section (i) of the Act, in order to determine the extent of the problem, and to find the most effective way to prevent recurrence of the problem.
- (8) Systems of Records - Review biennially each system of records notice to ensure that it accurately describes the system of records. Where minor changes are needed, e.g., the name of the system manager, ensure that an amended notice is published in the Federal Register. Agencies may choose to make one annual comprehensive publication consolidating such minor changes. This requirement is distinguished from and in addition to the requirement to report to OMB and Congress significant changes to systems of records and to publish those changes in the Federal Register (See paragraph 4c of this Appendix).
- (h) CNCS will assure that the use of new information technologies sustains, and does not erode, the protections provided in all statutes relating to Corporation use, collection, and disclosure of personal information;.
- (i) OIT will meet regularly with the CNCS Office of the Inspector General (OIG) to ensure that the program satisfies audit requirements.

5. ROLES & RESPONSIBILITIES:

- (a) The Chief Executive Officer (CEO) is responsible for:
 - (1) Provide executive support to promote information privacy throughout the Corporation.
 - (2) Assign a Senior Agency Official for Privacy
 - (3) Provide resources for the effective implementation of the privacy program

- (b) The Senior Agency Official for Privacy will:
- (1) Oversee, coordinate and facilitate Corporation compliance with privacy laws, regulations and policies, including maintaining appropriate documentation of compliance and ensuring remedial action for identified compliance weaknesses
 - (2) Assume a central policy-making role in the Corporation's development and evaluation of legislative, regulatory and other policy proposals which implicate information privacy
 - (3) Report and advise the CEO regarding the information privacy program
 - (4) Ensure the Corporation's employees and contractors receive appropriate training and education programs regarding the information privacy laws, regulations, policies, and procedures governing the Corporation's handling of personal information.
 - (5) Participate in assessing the impact of technology on the privacy of personal information.
- (c) The Privacy Officer (PO) is responsible for:
- (1) Developing and maintaining the CNCS information privacy program;
 - (2) Serving as the focal point for reporting and tracking all privacy related findings and corrective measures identified by any audit, review, scanning, or risk assessments conduct by the IG, OIT, or any other Federal agency directed to conduct such audits and reviews.
 - (3) Participating in the development of privacy-related reports to OMB and other oversight organizations.
- (d) The Chief Information Security Officer (CISO) is responsible for ensuring integration and coordination of the information privacy program with the information security program.
- (e) The Privacy Act Officer will:
- (1) Perform Privacy Act mandate reviews (as discussed above)
 - (2) Contribute to Corporation reporting on Privacy Act compliance.

6. DEFINITIONS:

- (a) Information Privacy - The preserving of an individual's right to significantly control the handling and access of information about themselves.
- (b) Metrics - Tools designed to facilitate decision-making and improve performance and accountability through collection, analysis, and reporting of relevant performance-related data.
- (c) Personally identifiable information (PII) - Information about an individual that identifies, links, relates, or is unique to, or describes him or her, or which can be used to distinguish or trace an individual's identity alone, or when combined with

other personal or identifying information. Examples include social security number; age; corporation assigned case number; email address; home/office phone number; driver's license ID number; biometric Record; finances; education; criminal history; physical attributes; gender, etc.

- (d) Plan of Actions and Milestones (POA&M) - A tool that identifies tasks that need to be accomplished. It details resources required to accomplish the elements of the plan, any milestones in meeting the task, and scheduled completion dates for the milestones. The purpose of this POA&M is to assist agencies in identifying, assessing, prioritizing, and monitoring the progress of corrective efforts for security weaknesses found in programs and systems.

7. ENFORCEMENT: Violation of this policy could result in loss or limitations on use of information resources, as well as disciplinary and/or legal action, including termination of employment and referral for criminal prosecution.

8. POINT OF CONTACT: CNCS Privacy Officer

9. ATTACHMENTS: None

10. AUTHORITY:

- (a) The Privacy Act of 1974, as amended, PL 93-579, December 31, 1974
- (b) Federal Information Security Management Act of 2002 (FISMA), PL 107-347, December 17, 2002
- (c) Section 208 of the E-Government Act of 2002 (44 U.S.C. § 3501 note)
- (d) OMB Memorandum M-05-08, Designation of Senior Agency Officials for Privacy, February 11, 2005.
- (e) OMB Memorandum M-03-22, OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002, September 30, 2003
- (f) OMB Circular A-130, Management of Federal Information Resources, Appendix III, Security of Federal Automated Information Resources, November 28, 2000.
- (g) OMB Memorandum M-99-05, Instructions on Complying with President's Memorandum of May 14, 1998, "Privacy and Personal Information in Federal Records" (January 7, 1999)
- (h) Government Paperwork Elimination Act (GPEA), PL 105-277, Title XVII, October 21, 1998.

- (i) Information Technology Management Reform Act of 1996 (also known as Clinger-Cohen Act; 41 U.S.C. § 251)
- (a) Freedom of Information Act of 1996 (FOIA)
- (b) OMB Circular A-123, "Management Accountability and Controls," June 21, 1995.
- (j) 5 CFR part 293, "Personnel Records," January 1, 2001
- (k) Privacy Act Implementation, Guidelines and Responsibilities, 40 FR 28948, July 9, 1975

11. EFFECTIVE DATE: September 15, 2008

12. REVISION HISTORY: None

13. REVIEW SCHEDULE: This policy will be reviewed and updated annually.

PRIVACY TRAINING AND AWARENESS

IPP-02-0808

1. **SUBJECT:** CNCS will implement a program to maintain awareness of information privacy policies, standards and acceptable practices.
2. **SCOPE:** This policy applies to all CNCS information users, including employees, contractors, interns, grantees, members, etc.
3. **DESCRIPTION:** Information Privacy is a continuous effort and "state of mind". This is achieved by reinforcing concerns and appropriate behaviors on an ongoing basis. Effective information privacy is achieved when it becomes part of everyone's thinking with regard to daily operations and assignments. Therefore, a Privacy Training and Awareness program is crucial to the effectiveness of the Information Privacy Program.
4. **PROCEDURES & GUIDELINES:**
 - (a) Information Privacy policies will be made available for reference and review by CNCS information users.
 - (1) Changes to CNCS Information Privacy policies or procedures will be communicated to all information users.
 - (2) CNCS will maintain and publish an Information Privacy Handbook.
 - (b) CNCS will provide training to all employees on their Privacy responsibilities.
 - (1) Information Privacy training will be incorporated into the orientation process for all new staff.
 - (2) Refresher and awareness training will be provided on at least an annual basis.
 - (3) Additional or advanced privacy training will be provided commensurate with roles and responsibilities.
 - (4) System Owners will provide system specific privacy training to the users of their systems.
 - (5) All employees responsible for the creation, development, maintenance, processing, use, dissemination, and safeguarding of personnel records will be trained on their responsibilities for handling of this type of information.
 - (c) Privacy training records will be maintained to document and monitor the training program and individuals' training activities.
 - (d) All staff will sign a Privacy Rules of Behavior agreement which establishes rules

of conduct when collecting and handling personal information, and the penalties for noncompliance. (See IPP-03, Rules and Consequences)

- (e) CNCS will operate an awareness program designed to focus attention on privacy, and to change behavior or reinforce good privacy practices. Ongoing development of privacy awareness builds a culture that encourages good privacy practices.

5. ROLES & RESPONSIBILITIES:

- (a) The Chief Executive Officer (CEO) is responsible for:
 - (1) Providing resources for training of staff
 - (2) Providing executive support for improving privacy awareness throughout the Corporation
- (b) The Privacy Officer (PO) is responsible for:
 - (1) Providing privacy training to staff
 - (2) Implementing processes and activities to promote privacy awareness
 - (3) Tracking privacy training and awareness activities.
- (c) The Office of Human Capital (OHC) will ensure that their own staff are provided additional privacy training and awareness related to handling of personnel information.
- (d) Information Owners are responsible for
 - (1) Ensuring that the users of their systems/information are aware of their privacy responsibilities when using those systems or handling that information.
 - (2) Providing system-specific privacy training
- (e) Supervisors are responsible for:
 - (1) Ensuring that their staff complete required privacy training
 - (2) Promoting privacy awareness within their staff
- (f) Information Users are responsible for:
 - (1) Completing privacy training when requested
 - (2) Maintaining awareness of their privacy responsibilities.

6. DEFINITIONS:

- (1) Privacy Awareness - A state of focused attention on privacy that allows individuals to recognize information privacy concerns and respond accordingly.

- 7. ENFORCEMENT:** Violation of this policy could result in loss or limitations on use of information resources, as well as disciplinary and/or legal action, including

termination of employment and referral for criminal prosecution.

8. POINT OF CONTACT: CNCS Privacy Officer

9. ATTACHMENTS: None

10. AUTHORITY:

- (a) The Privacy Act of 1974, as amended, PL 93-579, December 31, 1974
- (b) Federal Information Security Management Act of 2002 (FISMA), PL 107-347, December 17, 2002
- (c) OMB Circular A-130, Management of Federal Information Resources, Appendix III, Security of Federal Automated Information Resources, November 28, 2000.
- (d) OMB Memorandum "Guidance on Protecting Federal Employee Social Security Numbers and Combating Identity Theft"
- (e) Privacy Act Implementation, Guidelines and Responsibilities, 40 FR 28948, July 9, 1975

11. EFFECTIVE DATE: September 15, 2008

12. REVISION HISTORY: None

13. REVIEW SCHEDULE: This policy will be reviewed and updated annually.

INFORMATION PRIVACY RULES AND CONSEQUENCES

IPP-03-0808

- 1. SUBJECT:** All staff at CNCS have a duty to protect personally identifiable information (PII) from loss or misuse.
- 2. SCOPE:** This policy applies to the handling and protection of PII by Corporation personnel or other individuals on behalf of the Corporation.
- 3. DESCRIPTION:** All CNCS employees have a duty to protect from loss or misuse information about an individual that is maintained by the Corporation. This policy sets forth CNCS rules of behavior for maintaining and protecting personally identifiable information (PII), as well as the consequences and corrective actions available for failure to follow these rules. PII includes, but is not limited to, Social Security Numbers (SSNs), dates of birth, medical and financial information about individuals, home addresses, and home telephone numbers.
- 4. PROCEDURES & GUIDELINES:**
 - (a) All personnel shall:
 - (1) Protect all Personally Identifiable Information (PII), including both electronic and paper records, in their custody from unauthorized disclosure, modification or destruction so that the security and confidentiality of the information is preserved.
 - (2) Use and disclose PII only as authorized, and as permitted by posted privacy policies and systems of record notices.
 - (3) Complete all requested privacy training and awareness activities on time.
 - (4) Sign an agreement to comply with CNCS information privacy policies (Privacy Rules of Behavior).
 - (5) Comply with all laws, federal requirements, and CNCS policies and procedures regarding handling of privacy data.
 - (6) Encrypt all PII they transmit and all PII that they download to mobile computers/devices in accordance with CNCS procedures.
 - (7) Report any suspected unauthorized disclosures of PII in accordance with CNCS Information Security incident reporting procedures.
 - (8) Fully cooperate with investigations into incidents involving PII.

5. ROLES & RESPONSIBILITIES:

- (a) The Privacy Officer (PO) is responsible for:
 - (1) Establishing and collecting Privacy Rules of Behavior agreements
- (b) Information Owners are responsible for:
 - (1) Implementing and maintaining security controls to protect PII
 - (2) Ensuring that all personnel who have access to the data are trained and are compliant with policies and procedures for safeguarding PII collected and maintained at CNCS.
- (c) Supervisors are responsible for:
 - (1) Ensuring their staff understand the rules and consequences, and sign the Rules of Behavior Agreement.
 - (2) Taking appropriate remedial action when their staff violate CNCS privacy policies.
- (d) Information Users are responsible for:
 - (1) Reading, understanding, and signing the Privacy Rules of Behavior agreement.
 - (2) Adhering to CNCS privacy policies
 - (3) Properly handling PII to which they have access
 - (4) Immediately reporting suspected incidents.
 - (5) Fully cooperating with incident investigations.

6. DEFINITIONS:

- (a) Personally Identifiable Information (PII) – Information about an individual that identifies, links, relates, or is unique to, or describes him or her, or which can be used to distinguish or trace an individual’s identity alone, or when combined with other personal or identifying information. Examples include social security number; age; corporation assigned case number; email address; home/office phone number; driver’s license ID number; biometric Record; finances; education; criminal history; physical attributes; gender, etc.
- (b) Privacy Incident - An occurrence that actually or potentially jeopardizes the confidentiality privacy information, or violates privacy policies, procedures, or laws.

7. ENFORCEMENT: Violation of this policy could result in loss or limitations on use of information resources, as well as disciplinary and/or legal action, including termination of employment and referral for criminal prosecution.

The consequences of violating the above rules of behavior in handling PII range from administrative to criminal in nature some of which are defined by the Privacy Act of 1974, as amended.

- (a) Any official who willfully maintains a Privacy Act system of records without meeting the publication requirements is subject to possible criminal penalties or administrative sanctions, or both.
- (b) Any person who knowingly and willfully requests or obtains any Privacy Act record concerning an individual from an agency under false pretenses shall be guilty of a misdemeanor and fined not more than \$5,000.
- (c) Any employee with possession of, or access to PII who willfully discloses the material in any manner to any person or agency not entitled to receive it, may be guilty of a misdemeanor and fined not more than \$5,000.
- (d) Employees may be subject to written reprimand, suspension, or removal under situations including, but not limited to:
 - (1) Failing to implement and maintain required information security controls for the protection of PII, regardless of whether such action results in the loss of control or unauthorized disclosure of PII.
 - (2) Failing to report any known or suspected loss of control over, or unauthorized disclosure of, PII.
 - (3) For managers, failing to adequately instruct, train, or supervise employees in their responsibilities.

8. POINT OF CONTACT: CNCS Privacy Officer

9. ATTACHMENTS: None

10. AUTHORITY:

- (a) The Privacy Act of 1974, as amended, PL 93-579, December 31, 1974
- (b) Federal Information Security Management Act of 2002 (FISMA), PL 107-347, December 17, 2002
- (c) OMB Circular A-130, Management of Federal Information Resources, Appendix III, Security of Federal Automated Information Resources, November 28, 2000.
- (d) OMB Memorandum M-07-16, Safeguarding against and Responding to the Breach of Personally Identifiable Information
- (e) Executive Order 13402, May 10, 2006, President's Identity Theft Task Force and the Task Force's report: Combating Identity Theft – A Strategic Plan, April 2007
- (f) OMB Memorandum M-06-16, Protection of Sensitive Agency Information

11. EFFECTIVE DATE: September 15, 2008

12. REVISION HISTORY: None

13. REVIEW SCHEDULE: This policy will be reviewed and updated annually.

PRIVACY INCIDENT MANAGEMENT

IPP-04-0808

1. **SUBJECT:** The Corporation must be able to respond to privacy-related incidents in a manner that protects its own information and helps to protect the information of others that might be affected by the incident.

2. **SCOPE:** This policy applies to all potential or actual breaches of privacy information.

3. **DESCRIPTION:** Data breaches can result in a broad range of harms to individuals, including identity theft. The crime of identity theft occurs when an individual's identifying information is used by another without authorization in an attempt to commit fraud or other crimes. Identity theft undermines consumer confidence, harms our economy, and wastes consumer time, money, and effort to correct the damage caused by an identity thief. Steps must be taken to mitigate the potential harm due to breach of personal information.

4. **PROCEDURES & GUIDELINES:**
 - (a) Privacy incidents will be reported and handled in accordance with CNCS' "Incident Reporting" (ISP-P-03) and "Incident Response" (ISP-P-04) policies.
 - (1) A CNCS Incident Response Report must be completed for all privacy incidents.
 - (2) A Missing IT Asset Impact Analysis must be completed for incidents involving loss of Corporation property.
 - (b) All incidents involving personally identifiable information are to be reported to US-CERT within one hour of discovering the incident. This includes both suspected and confirmed breaches.
 - (c) If at any time the loss of data was intentional or data was the target of the incident, OIG must be notified.
 - (d) The Corporation will establish a core Privacy Incident Response Team (PIRT) responsible for responding to the loss of personal information.
 - (e) If an incident occurs, the PIRT will engage in a risk analysis to determine whether the incident poses risks related to identity theft. The Corporation will then tailor its response to the nature and scope of the risk presented.
 - (1) If the incident results in a risk of identity theft to the person(s) whose data has been breached, the Corporation will provide credit monitoring advice to the

person(s) and may offer additional services to resolve the situation if warranted.

- (f) The Corporation will provide timely notification to anyone whose personal information has been breached while under the care of the Corporation or its contractors on behalf of the Corporation.
 - (1) The notification must be made in such a way as to not further violate the privacy of the person(s) affected.
 - (2) The manner of notification will be customized to the particular situation of the incident.
 - (3) A point of contact will be designated and provided as part of the notification.
- (g) The Corporation will establish formal procedures into a plan for addressing breaches of privacy information.
- (h) If mitigation services are offered to affected individuals, the government-wide blanket purchase (BPA) will be utilized. For services other than those provided by the GSA BPA, the purchaser shall send a notice to GSA and to the OMB E-Government Administrator, identifying the pricing and terms and conditions of the award. Notices shall be prepared in coordination with CNCS' Acquisition Officer and the Chief Information Officer and submitted at least 10 days prior to making an award, except in the event of unusual and compelling urgency, in which case the notice shall be provided as soon as practicable.

5. ROLES & RESPONSIBILITIES:

- (a) The Senior Agency Official for Privacy (SAOP) is responsible for:
 - (1) Reporting incidents to executive management.
 - (2) Participating in the Privacy Incident Response Team
 - (3) Ensuring that incidents are reported as required by OMB.
- (b) The Privacy Officer (PO) is responsible for:
 - (1) Developing and maintaining procedures for reporting and responding to breaches of privacy information.
 - (2) Reporting privacy incidents to US-CERT.
 - (3) Activating the CNCS Privacy Incident Remediation Team.
 - (4) Preparing privacy incident reports.
 - (5) Participating in incident response activities.
- (c) The Chief Information Security Officer (CISO) will:
 - (1) Participate in the Privacy Incident Response Team.
 - (2) Manage the information security incident response process and coordinate with the privacy officer for incidents involving privacy information.

- (d) Information Owners are responsible for:
 - (1) Ensuring that incidents involving their information and systems are reported immediately and that an Incident Response Report (and *Missing IT Asset Impact Analysis* if required) is prepared.
 - (2) Ensuring that a routine use has been developed and published allowing for the disclosure of information in the course of responding to a breach.
 - (3) Providing notification and assistance to affected individuals as determined by the PIRT.
- (e) Supervisors are responsible for:
 - (1) Ensuring that their staff understand their responsibilities regarding reporting of incidents
 - (2) Ensuring full cooperation from their staff for investigation and resolution of incidents.
- (f) Information Users are responsible for:
 - (1) Immediately reporting potential incidents
 - (2) Providing requested incident reports and other supporting materials.
 - (3) Fully cooperating with incident investigations.

6. DEFINITIONS:

- (a) Information Privacy - The preserving of an individual's right to significantly control the handling and access of information about themselves.
- (b) Personally Identifiable Information (PII) – Information about an individual that identifies, links, relates, or is unique to, or describes him or her, or which can be used to distinguish or trace an individual's identity alone, or when combined with other personal or identifying information. Examples include social security number; age; corporation assigned case number; email address; home/office phone number; driver's license ID number; biometric Record; finances; education; criminal history; physical attributes; gender, etc.
- (c) Privacy Incident - An occurrence that actually or potentially jeopardizes the confidentiality of privacy information, or violates privacy policies, procedures, or laws.

7. ENFORCEMENT: Violation of this policy could result in loss or limitations on use of information resources, as well as disciplinary and/or legal action, including termination of employment and referral for criminal prosecution.

8. POINT OF CONTACT: CNCS Privacy Officer

9. ATTACHMENTS: None

10. AUTHORITY:

- (a) The Privacy Act of 1974, as amended, PL 93-579, December 31, 1974
- (b) Federal Information Security Management Act of 2002 (FISMA), PL 107-347, December 17, 2002
- (c) OMB Memorandum M-07-16, Safeguarding Against and Responding to the Breach of Personally Identifiable Information, May 22, 2007.
- (d) OMB Memorandum M-07-04, Use of Commercial Credit Monitoring Services Blanket Purchase Agreements (BPA), December 22, 2006.
- (e) OMB Memorandum M-06-19, Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments, July 12, 2006
- (f) OMB Memorandum, Recommendations for Identity Theft Related Data Breach Notification, September 20, 2006
- (g) Identity Theft Task Force, Combating Identity Theft: A Strategic Plan, April 2007
- (h) OMB Circular A-130, Management of Federal Information Resources, Appendix III, Security of Federal Automated Information Resources, November 28, 2000.

11. EFFECTIVE DATE: September 15, 2008

12. REVISION HISTORY: None

13. REVIEW SCHEDULE: This policy will be reviewed and updated annually.

COLLECTING AND PROTECTING PERSONAL INFORMATION

IPP-05-0808

1. **SUBJECT:** CNCS will implement appropriate safeguards and procedures when collecting, storing, and handling personal information in order to protect individuals' privacy rights.
2. **SCOPE:** This policy applies to all personally identifiable information collected or handled by the Corporation.
3. **DESCRIPTION:** The loss of Personally Identifiable Information (PII) can result in substantial harm, embarrassment, and inconvenience to individuals and may lead to identity theft or other fraudulent use of the information. Because Federal agencies maintain significant amounts of information concerning individuals, we have a special duty to protect that information from loss and misuse. The Corporation has many responsibilities under law to appropriately safeguard PII.
4. **PROCEDURES & GUIDELINES:**
 - (a) CNCS will evaluate proposals involving collection, use and disclosure of personal information for consistency with the Privacy Act of 1974.
 - (b) CNCS will collect only the information necessary and managing it properly to reduce risk to the information and the burden of safeguarding it.
 - (1) The Corporation will minimize the use of social security numbers in agency systems and programs.
 - (2) The Corporation will eliminate the use of social security numbers as a record identifier.
 - (c) CNCS will establish appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of records and to protect against any anticipated threats or hazards to their security or integrity which could result in substantial harm, embarrassment, inconvenience or unfairness to any individual on whom information is maintained.
 - (d) PII will be safeguarded in accordance with the requirements of FISMA, OMB, NIST, and CNCS Information Security policies.
 - (1) Personal information will protected as "sensitive information" under Corporation Information Security policies.
 - (e) CNCS will identify systems of records and develop and publish notices as required by the Privacy Act and OMB's implementing policies. (See IPP-07 Systems Of Records)
 - (f) The Corporation will periodically review its holdings of all PII and ensure, to the maximum extent practicable, such holdings are accurate, relevant, timely, and complete, and reduce them to the minimum necessary for the proper performance of a documented agency function.

- (g) CNCS will not rent or sell information about individuals.
- (h) CNCS will only disclose privacy information in accordance with routine uses published in the system of records notice or as directed by law. (See IPP-07 Systems of Records)
- (i) All disclosures of information containing Social Security Numbers and other personally identifiable data must be made in accordance with established regulations and procedures.
- (j) All extracts of personal information from Corporation systems will be logged and verified in accordance with IPP-10 Data Extracts.
- (k) If CNCS or its contractors receive data transferred from the private sector, the Corporation will ensure the same protections and compliance with the Privacy Act as if the data was originally collected by the Corporation. This includes publication of a System of Records Notice.
- (l) Agencies may not require individuals to disclose their Social Security Number (SSN) unless disclosure would be required under a Federal statute; or any statute, Executive order, or regulation that authorizes any Federal, State, or local agency maintaining a system of records that was in existence and operating prior to January 1, 1975, to request the SSN as a necessary means of verifying the identity of an individual.
- (m) Individuals asked to voluntarily provide their SSN shall suffer no penalty or denial of benefits for refusing to provide it.
- (n) CNCS will eliminate the unnecessary printing and displaying of SSNs on forms, reports, and computer display screens.
- (o) Access to SSNs will be restricted to only those individuals whose official duty requires such access. A listing of all access authorizations should be maintained and monitored regularly for continued applicability.
- (p) Those individuals who are authorized to access the SSN must understand their responsibility to protect sensitive and personal information. This includes securing this information when working from home or another remote location.
- (q) Supervisory approval is required before an authorized individual can access, transport, or transmit information or equipment containing Social Security Numbers outside agency facilities.
- (r) Electronic records containing Social Security Numbers should be transported or transmitted in an encrypted or protected format as prescribed in current OMB guidance regarding the protection of sensitive agency information.
- (s) Paper-based records containing Social Security Numbers should be transported in wheeled containers, portfolios, briefcases, or similar devices that are locked when the records are not in use. These containers should be identifiable by tag, label, or decal with contact and mailing information.
- (t) Managers of automated personnel records shall establish administrative, technical, physical, and security safeguards for data about individuals in automated records, including input and output documents, reports, punched cards, magnetic tapes, disks, and on-line computer storage.
- (u) Collecting and handling employee Social Security Numbers:

- (1) If Social Security Numbers are collected, they should be collected at the time of an employee's appointment and entered into the human resources and payroll systems.
- (2) The collection tool (if paper-based) should be stored in a secure location until it is no longer required. Disposal of all paper-based collection tools (i.e., forms, letters, and other correspondence) must be in accordance with the General Record Schedule issued by the National Archives and Records Administration.
- (3) Privacy and confidentiality statements that describe accountability clearly and warn of possible disciplinary action for unauthorized release of the Social Security Number and other personally identifiable information should be signed by all individuals who have access to the Social Security Number.
- (4) Agency Telework policies and written agreements must be in compliance with Federal privacy protection policies, including policies governing the protection of employee Social Security Numbers.
- (5) Required access to Social Security Numbers, including data entry, printing, and screen displays must be conducted in a secure location to protect against unauthorized exposures.
- (6) When the Social Security Number is required as a data entry parameter, it must not be displayed on the input screen except when establishing the initial human resources or payroll record. In all other record retrieval and access authorization processes, the Social Security Number must be masked with asterisks or other special characters, similar to the technique used when handling passwords and PINs.
- (7) Adequate internal control procedures must be employed to ensure the proper monitoring of authorized and unauthorized access to Social Security Numbers and other personally identifiable information.

5. ROLES & RESPONSIBILITIES:

- (a) The Privacy Officer (PO) is responsible for:
 - (1) Providing guidance on collection and handling of personal information
 - (2) Auditing to ensure compliance with CNCS privacy policies.
- (b) Information Owners are responsible for:
 - (1) Collecting and handling personal information in accordance with CNCS policies and federal requirements.
 - (2) Protecting all personal information in systems that they own.
- (c) Information Users are responsible for:
 - (1) Handling personal information in accordance with CNCS policies and federal requirements.

6. DEFINITIONS:

- (a) Data Extract - Data retrieved from a database through a query and saved into a separate computer-readable entity such as another database, a spreadsheet, or a text file
- (b) Personally Identifiable Information - Information about an individual that identifies, links, relates, or is unique to, or describes him or her, or which can be used to distinguish or trace an individual's identity alone, or when combined with other personal or identifying information. Examples include social security number; age; corporation assigned case number; email address; home/office phone number; driver's license ID number; biometric Record; finances; education; criminal history; physical attributes; gender, etc.
- (c) Routine Use – A disclosure of a record outside of the agency "for a purpose which is compatible with the purpose for which it was collected."
- (d) 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 the individual

7. ENFORCEMENT: Violation of this policy could result in loss or limitations on use of information resources, as well as disciplinary and/or legal action, including termination of employment and referral for criminal prosecution.

8. POINT OF CONTACT: CNCS Privacy Officer

9. ATTACHMENTS: None

10. AUTHORITY:

- (a) The Privacy Act of 1974, as amended, PL 93-579, December 31, 1974
- (b) OMB Memorandum M-06-16, Protection of Sensitive Agency Information, June 23, 2006
- (c) OMB Memorandum M-06-15, Safeguarding Personally Identifiable Information, May 22, 2006
- (d) OMB Memorandum "Guidance on Protecting Federal Employee Social Security Numbers and Combating Identity Theft"
- (e) OMB Memorandum M-99-05, Instructions on Complying with President's Memorandum of May 14, 1998, "Privacy and Personal Information in Federal Records" (January 7, 1999)

- (f) Federal Information Security Management Act of 2002 (FISMA), PL 107-347, December 17, 2002
- (g) OMB Circular A-130, Management of Federal Information Resources, Appendix III, Security of Federal Automated Information Resources, November 28, 2000.
- (h) Government Paperwork Elimination Act (GPEA), PL 105-277, Title XVII, October 21, 1998.
- (i) Privacy Act Implementation, Guidelines and Responsibilities, 40 FR 28948, July 9, 1975

11. EFFECTIVE DATE: September 15, 2008

12. REVISION HISTORY: None

13. REVIEW SCHEDULE: This policy will be reviewed and updated annually.

PRIVACY IMPACT ASSESSMENTS

IPP-06-0808

- 1. SUBJECT:** CNCS must conduct Privacy Impact Assessments (PIAs) before developing, procuring, or substantially modifying information technology (IT) projects or systems that collect, maintain, or disseminate information in identifiable form (IIF) and make those PIAs publicly available.
- 2. SCOPE:** This policy applies to all IT projects and systems owned by or operated on behalf of CNCS.
- 3. DESCRIPTION:** Privacy Impact Assessment (PIA) is a process for determining the risks and effects of collecting, maintaining, and disseminating information in identifiable form (IIF) in an electronic information system, and for identifying and evaluating protections and alternative processes to mitigate the impact to privacy of collecting the information.

PIAs are conducted to ensure that there is no collection, storage, access, use, or dissemination of identifiable information from or about members of the general public and businesses that is not needed or authorized, and that identifiable information that is collected is adequately protected. PIAs may address issues relating to the integrity and availability of data handled by a system, to the extent these issues are not already adequately addressed in a System Security Plan prepared in accordance with the CNCS IT security policy.

4. PROCEDURES & GUIDELINES:

- (a) CNCS will conduct privacy impact assessments (PIAs) for electronic information systems and collections and make them publicly available.
- (b) CNCS will designate an appropriate official (or officials) to serve as the “reviewing official(s)” for agency PIAs.
- (c) PIAs will be performed and updated as necessary whenever a system change creates new privacy risks.
 - (1) CNCS will conduct a PIA before:
 - developing or procuring IT systems or projects that collect, maintain or disseminate IIF from or about members of the public
 - initiating a new collection of IIF that will be collected, maintained, or disseminated using information technology, for 10 or more persons (excluding agencies, instrumentalities or employees of the federal government).

- Newly applying user-authenticating technology (e.g., password, digital certificate, biometric) to an electronic information system accessed by members of the public.
 - Systematically incorporating into existing information systems any databases of IIF purchased or obtained from commercial or public sources.
 - Working together with other agencies on shared functions involving significant new uses or exchanges of IIF, such as the cross-cutting E-Government initiatives.
 - Altering a business process, resulting in significant new uses or disclosures of information or incorporation into the system of additional items of IIF:
 - Altering the character of data - when new IIF added to a collection raises the risks to personal privacy (for example, the addition of health or financial information)
- (2) PIAs should be conducted when developing, or issuing a change to, a System of Records Notice.
- (3) CNCS will update its PIAs to reflect changed information collection authorities, business processes or other factors affecting the collection and handling of IIF.
- (d) PIAs will analyze and describe:
- (1) what information is to be collected.
 - (2) why the information is being collected.
 - (3) intended use of the information (e.g., to verify existing data).
 - (4) with whom the information will be shared and why.
 - (5) what opportunities individuals have to decline to provide information (when providing information is voluntary) or to consent to particular uses of the information (other than required or authorized uses), and how individuals can grant consent.
 - (6) how the information will be secured (e.g., administrative and technological controls).
 - (7) whether a system of records is being created under the Privacy Act.
 - (8) what choices the agency made regarding an IT system or collection of information as a result of performing the PIA.
- (e) The depth and content of the PIA should be appropriate for the nature of the information to be collected and the size and complexity of the IT system.
- (1) PIAs conducted for Major information systems should reflect more extensive analyses of:

- the consequences of collection and flow of information.
 - the alternatives to collection and handling as designed.
 - the appropriate measures to mitigate risks identified for each alternative.
 - the rationale for the final design choice or business process.
- (f) The PIA document must be approved by the CNCS “reviewing official”.
- (g) The PIA document or a summary will be made publicly available (consistent with executive branch policy on the release of information about systems for which funding is proposed) unless that publication would raise security concerns, reveal classified (i.e., national security) information or sensitive information (e.g., potentially damaging to a national interest, law enforcement effort or competitive business interest) contained in an assessment. Such information is protected and handled consistent with the Freedom of Information Act (FOIA).
- (1) No actual privacy data (such as IIF) will be included in the PIA.
- (h) CNCS will consider the information “life cycle” (i.e., collection, use, retention, processing, disclosure and destruction) in evaluating how information handling practices at each stage may affect individuals’ privacy.
- (i) To be comprehensive and meaningful, PIAs require collaboration by program experts as well as experts in the areas of information technology, security, records management and privacy.

5. ROLES & RESPONSIBILITIES:

- (a) The Privacy Officer (PO) is responsible for:
- (1) Providing guidance to Corporation personnel on the conducting and updating of PIAs.
 - (2) Developing and maintaining PIA templates and procedures.
 - (3) Maintaining an inventory and repository of Corporation PIAs.
- (b) Information Owners are responsible for:
- (1) Conducting and updating PIAs on any information and systems that they own as required by this policy.
 - (2) Providing completed PIAs to the agency "reviewing official" for approval.
 - (3) Ensuring that information collections and systems are maintained in compliance with the requirements documented in their PIAs.
 - (4) Posting approved PIAs in accordance with CNCS PIA posting procedures.
 - (5) Providing copies of approved PIAs to the Privacy Officer.
- (c) The "reviewing official" is responsible for reviewing and approving PIAs.

6. DEFINITIONS:

- (a) Information in Identifiable Form (IIF) - Information in an IT system or online collection: (i) that directly identifies an individual (e.g., name, address, social security number or other identifying number or code, telephone number, email address, etc.) or (ii) by which an agency intends to identify specific individuals in conjunction with other data elements, i.e., indirect identification. These data element may include a combination of gender, race, birth date, geographic indicator, and other descriptors.
- (b) Information Privacy - The preserving of an individual's right to significantly control the handling and access of information about themselves.
- (c) Information Technology (IT) – Any equipment, software or interconnected system or subsystem that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information.
- (d) Personally Identifiable Information (PII) – Information about an individual that identifies, links, relates, or is unique to, or describes him or her, or which can be used to distinguish or trace an individual's identity alone, or when combined with other personal or identifying information. Examples include social security number; age; corporation assigned case number; email address; home/office phone number; driver's license ID number; biometric Record; finances; education; criminal history; physical attributes; gender, etc.
- (e) Privacy Impact Assessment (PIA) – An analysis of how information is handled: (i) to ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy, (ii) to determine the risks and effects of collecting, maintaining and disseminating IIF in an electronic information system, and (iii) to examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risk.

7. ENFORCEMENT: Violation of this policy could result in loss or limitations on use of information resources, as well as disciplinary and/or legal action, including termination of employment and referral for criminal prosecution.

8. POINT OF CONTACT: CNCS Privacy Officer

9. ATTACHMENTS: None

10. AUTHORITY:

- (a) The Privacy Act of 1974, as amended, PL 93-579, December 31, 1974
- (b) Federal Information Security Management Act of 2002 (FISMA), PL 107-347, December 17, 2002

- (c) OMB Circular A-130, Management of Federal Information Resources, Appendix III, Security of Federal Automated Information Resources, November 28, 2000.
- (d) OMB Memorandum M-03-22, OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002, September 30, 2003

11. EFFECTIVE DATE: September 15, 2008

12. REVISION HISTORY: None

13. REVIEW SCHEDULE: This policy will be reviewed and updated annually.

SYSTEMS OF RECORDS

IPP-07-0808

1. **SUBJECT:** CNCS will publish notices for its systems of records in accordance with Privacy Act requirements, and will periodically review them to ensure that they are accurate and complete.
2. **SCOPE:** This policy applies to all systems of records, both electronic and paper, that contain personally identifiable information (PII).
3. **DESCRIPTION:** The Privacy Act of 1974 (5 U.S.C. § 552a, the Act) requires agencies to inform the public of the existence of Systems of Records containing personal information, to give individuals access to records about themselves in a system of records, and to manage those records in a way to ensure fairness to individuals in agency programs.

For the Privacy Act to work effectively, it is imperative that each agency properly maintain its systems of records and ensure that the public is adequately informed about the systems of records the agency maintains and the uses that are being made of the records in those systems. Therefore, agencies must periodically review their systems of records and the published notices that describe them to ensure that they are accurate and complete.

4. PROCEDURES & GUIDELINES:

- (a) CNCS will identify each system of records which the agency maintains and will review the contents of the system to assure that only necessary information relevant to the Corporation's mission is maintained.
 - (1) Information about political or religious beliefs and activities of individuals will not be maintained.
- (b) A System of Records Notice (SORN) must be developed for each System of Records containing personal information. The core purpose of a SORN is to inform the public what types of records the agency maintains, who the records are about, and what uses are made of them.
 - (1) The Corporation will publish a SORN upon the establishment or alteration of a system of records.
 - (2) SORNs will be published in the Federal Register.
 - (3) Each SORN will include:
 - Name and location of the system.

- Categories of individuals on whom records are maintained in the system.
 - A statement of what types of information are maintained and what the sources of the information are.
 - Each routine use of records contained in the system, including the categories of users and the purpose of such use.
 - Policies and practices of the agency regarding storage, retrievability, access controls, retention, and disposal of the records.
 - Title, name, and business address of the agency official who is responsible for the system of records (This field requires the name of an individual and not just the title)
 - Agency procedures to notify an individual, at his request, how he can gain access to any record pertaining to him contained in the system of records, and how (s)he can contest its content.
- (c) Systems of Records and their corresponding notices will be reviewed and updated periodically. SORN reviews will include:
- (1) Verifying that a SORN exists for each system of records.
 - (2) Ensuring that each system of records contains only that information about individuals that is "relevant and necessary" to accomplish an agency purpose.
 - (3) Verifying that the original purpose justifying the information collection is still relevant.
 - (4) Ensuring that each SORN accurately and completely describes the routine uses, including the categories of users and the purpose of such use.
 - (5) Reviewing each routine use to ensure that it continues to be appropriate.
 - (6) Checking if changes in agency operations or functions have resulted in increased differences among the records that are contained within a common system of records or groups of records that once were appropriately combined into a common system may have become sufficiently different that they should be divided into separate systems.
 - (7) If it is determined that the SORN does not accurately and completely describe the system of records and its routine uses, the Corporation will revise the notice accordingly.
- (d) If any information about individuals in a system of records is no longer relevant and necessary, or if the entire system of records itself is no longer relevant and necessary, then the Corporation will expunge the records (or system of records) in accordance with the procedures outlined in the Privacy Act notice(s) and the prescribed record retention schedule approved by the National Archives and Records Administration.
- (1) The SORN will be accordingly revised (or rescinded).
- (e) The Corporation will ensure that its systems of records do not inappropriately combine groups of records which should be segregated. "Groups of records which have different purposes, routine uses, or security requirements, or which are regularly accessed by different members of the agency staff, should be maintained and managed as separate systems of records to avoid lapses in security."¹

¹ M-99-05

- (f) The Corporation will ensure the security and confidentiality of the personal information in the system of records.
- (1) Personal information will be treated as "sensitive information" under the CNCS information security policies.
 - (2) Personal information will be protected in accordance with IPP-05 Collecting and Protecting Personal Information.
 - (3) Safeguards will be reviewed annually to ensure that they are appropriate, and will be updated if necessary.
 - (4) If changes to the safeguards are made, then the Corporation will publish a system of records notice that reflects the updated safeguards.
 - The notice should explain *how* access is limited by describing the types of safeguards in place, such as locks, building access controls, passwords, network authentication, etc.
- (g) Routine Uses
- (1) Non-statutory disclosures created by administrative mechanisms should only be made when appropriate.
 - (2) CNCS will periodically review its "routine uses" to identify any routine uses that are no longer justified, or which are no longer compatible with the purpose for which the information was collected.
 - (3) If a routine use is no longer appropriate, the agency should discontinue the routine-use disclosures and delete the routine use from the system of records notice.
 - (4) If the system of records notice does not accurately and completely describe the routine uses, the notice must be updated accordingly.
 - (5) General routine uses that should be added to all SORNs include:
 - Disclosure for Law Enforcement Purposes - Information from this system of records may be disclosed to appropriate Federal, State, local agencies, or other public entities responsible for investigating, prosecuting, enforcing, or implementing a statute, rule, regulation, or order, if the information is relevant to a violation or potential violation of civil or criminal law or regulation within the jurisdiction of the receiving entity.
 - Disclosure Incident to Requesting Information - Information from this system of records may be disclosed to any source from which additional information is requested (to the extent necessary to identify the individual, inform the source of the purpose of the request, and to identify the type of information requested), when necessary to obtain information relevant to a CNCS decision concerning retention of an employee or other personnel action (other than hiring), retention of a security clearance, the letting of a contract, or the issuance or retention of a grant, or other benefit.
 - Disclosure to Requesting Agencies - Disclosure from this system of

records may be made to Federal, State, local, or other public authorities of the fact that this system of records contains information relevant to the retention of an employee, the retention of a security clearance, the letting of a contract, or the obtaining, retaining, or issuing of a license, grant, or other benefit. The other agency or licensing organization may then make a request supported by the written consent of the individual for the entire record if it so chooses. No disclosure will be made unless the information has been determined to be sufficiently reliable to support a referral to another office within the agency or to a Federal agency or state or local agency or other public body for criminal, civil, administrative, personnel, or regulatory action.

- Disclosure to Congressional Offices - Information from this system of records may be disclosed to congressional offices in response to inquiries from congressional offices or offices of the elected officials made at the request of such individuals.
- Disclosure to Courts or Administrative Bodies - Information from this system of records may be disclosed in proceedings before courts, adjudicative bodies, or other administrative bodies before which CNCS is authorized to appear or which have oversight authority over CNCS when the use of such records is deemed to be relevant and necessary to the litigation, investigation or audit, provided, however, that in each case it has been determined that the disclosure is compatible with the purpose for which the records were collected.
- Disclosure to Contractors, Grantors, Grantees, Federal Government Agencies, and Others - Information from this system of records may be disclosed to contractors, grantees, the Federal Government, consultants, volunteers or other parties performing or working on a contract, service, grant, cooperative agreement, memorandum of understanding, job, or other activity on behalf of CNCS and who have a need to have access to the information in the performance of their duties or activities for CNCS, which need should be related to the purpose for which the record is maintained. When appropriate, recipients will be required to comply with the requirements of the Privacy Policy.
- Disclosures for Administrative Claims, Complaints, and Appeals - Information from this system of records may be disclosed to authorized appeal grievance examiners, formal complaints examiners, equal employment opportunity investigators, arbitrators or other persons properly engaged in investigation or settlement of administrative grievances, complaints, claims, or appeals filed by employees, but only to the extent that the information is relevant and necessary to the proceedings. Agencies that may obtain information under this routine use include, but are not limited to, the and Equal Employment Opportunity Commission and the Department of Labor.

- Disclosure in Connection with Litigation - Information from this system of records may be disclosed in connection with litigation or settlement discussions regarding claims by or against CNCS, including public filings with courts, to the extent that disclosure of the information is relevant and necessary to the litigation or discussions and except where court orders are otherwise required.
 - Disclosure to the Government Accountability Office (GAO), Office of Management and Budget (OMB), or Other Government Oversight Agencies - Information from this system of records may be disclosed to the GAO, OMB or other government oversight agencies pursuant to their responsibility for evaluation and oversight of CNCS.
- (h) The Corporation will "keep an accurate accounting" regarding "each disclosure of a record to any person or to another agency, "and [will] retain the accounting for at least five years or the life of the record, whichever is longer."² . This includes those made under routine uses, and those made pursuant to requests from law enforcement agencies (even though the latter may be exempt from disclosures to the subject individual).
- (1) Exceptions are made for disclosures made within the agency on a need-to-know basis or disclosure required by the Freedom of Information Act.
- (2) The accounting process must be periodically reviewed and updated to ensure effectiveness. This includes reviewing "changes in technology, function, and organization" that may result in accounting procedures becoming outdated or inadequate.
- (3) The accounting will include at least the following:
- Date of disclosure
 - Nature, and purpose of each disclosure
 - Name and address of person to whom the data was disclosed
- (4) The account must be made even if it is at the request or authorization of the individual.
- (i) When using or disclosing a record, CNCS will assure that it is as accurate, relevant, timely, and complete as is reasonably necessary to ensure fairness to the individual.
- (j) Corporation systems of records should not duplicate or be combined with those systems which have been designated as "government wide systems of records." A government wide system of records is one for which one agency has regulatory authority over records in the custody of many different agencies. Usually these are federal personnel or administrative records. Such government-wide systems ensure that privacy practices with respect to those records are carried out in accordance with the responsible agency's regulations uniformly across the federal

² 5 U.S.C. § 552a(c)

government."

- (k) Individuals will be notified of the purposes for which their information is collected, and of their rights and obligations regarding supplying the data, at the time of collection
- (l) CNCS will permit individuals access to records pertaining to themselves to request amendments to those records.
 - (1) Upon request from an individual, CNCS will:
 - Inform the individual whether a system of records contains records to pertaining to them.
 - Permit the individual to the review any record retrieved by reference to themselves contained in a system of records. (This does not pertain to records referenced under someone else's name which include mention of the individual).
 - Permit the individual to obtain a copy of any such record at reasonable cost.
 - (2) Upon receipt of a request from an individual to amend their record, CNCS will:
 - Acknowledge receipt of the request in writing within 10 working days and advise the individual of when action will be taken on the request.
 - Make corrections to any portion of the information that the individual believes is inaccurate or inform the individual of its refusal to amend the records and the reason for refusal.
- (m) CNCS will review all agency contracts which provide for maintenance of a system of records on behalf of the Corporation to ensure that Privacy Act requirements are included.
- (n) CNCS will assure that personal information contained in Privacy Act systems of records be handled in full compliance with fair information practices as set out in the Privacy Act of 1974

5. ROLES & RESPONSIBILITIES:

- (a) The Privacy Officer (PO) is responsible for:
 - (1) Provide guidance and review for developing SORNs
 - (2) Audit to ensure that SORNs are complete, accurate, and in place for all required systems.
 - (3) Inventory and report on SORNs.
- (b) Information Owners are responsible for:
 - (1) Ensuring that only necessary and relevant information is collected in their

systems of records.

- (2) Ensuring that the information is only used and shared in accordance with the description in the SORN and in compliance with legal requirements.
 - (3) Developing, periodically reviewing, and updating notices for their systems of records.
 - (4) Ensuring that appropriate safeguards are applied to protect the information in their systems of records.
 - (5) Securely decommissioning the system of records when it is no longer required.
 - (6) Ensuring the accuracy of personal information held in a system of records.
 - (7) Responding to access and correction requests from individuals regarding their personal information held by the Corporation.
- (c) The Office of General Counsel is responsible for posting provided SORNs to the Federal Register.

6. DEFINITIONS:

- (a) Disclosure - Release of information contained in a system of records to any person (other than the person to whom the information pertains), including any employee of CNCS, or employees of other Federal agencies.
- (b) Personally Identifiable Information - Information about an individual that identifies, links, relates, or is unique to, or describes him or her, or which can be used to distinguish or trace an individual's identity alone, or when combined with other personal or identifying information. Examples include social security number; age; corporation assigned case number; email address; home/office phone number; driver's license ID number; biometric Record; finances; education; criminal history; physical attributes; gender, etc.
- (c) Record - Any item, collection, or grouping of information about an individual that is maintained by an agency and contains his or her name or another personal identifier. This includes, but not limited to, his education, financial transactions, medical history, and criminal or employment history and that contains his name, or the identifying number, symbol, or other identifying particular assigned to the individual, such as a finger or voice print or a photograph
- (d) Routine Use – A disclosure of a record outside of the agency "for a purpose which is compatible with the purpose for which it was collected."
- (e) 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 the individual

7. ENFORCEMENT: Violation of this policy could result in loss or limitations on use

of information resources, as well as disciplinary and/or legal action, including termination of employment and referral for criminal prosecution.

8. POINT OF CONTACT: CNCS Privacy Officer

9. ATTACHMENTS: None

10. AUTHORITY:

- (a) The Privacy Act of 1974, as amended, PL 93-579, December 31, 1974
- (b) Federal Information Security Management Act of 2002 (FISMA), PL 107-347, December 17, 2002
- (c) OMB Circular A-130, Management of Federal Information Resources, Appendix III, Security of Federal Automated Information Resources, November 28, 2000.
- (d) OMB Memorandum M-99-05, Instructions on Complying with President's Memorandum of May 14, 1998, "Privacy and Personal Information in Federal Records" (January 7, 1999)
- (e) Privacy Act Implementation, Guidelines and Responsibilities, 40 FR 28948, July 9, 1975

11. EFFECTIVE DATE: September 15, 2008

12. REVISION HISTORY: None

13. REVIEW SCHEDULE: This policy will be reviewed and updated annually.

WEB SITE PRIVACY

IPP-08-0808

1. **SUBJECT:** CNCS must protect an individual's right to privacy when personal information is collected on Corporation web sites.
2. **SCOPE:** This policy applies to all web sites hosted by or on behalf of the Corporation which are accessible by the public.
3. **DESCRIPTION:** "Web sites are a powerful tool for conveying information on topics relating to activities, objectives, policies and programs of the Federal Government. Web pages provide a simple and speedy means of gaining access to information about the Government, thereby increasing knowledge and understanding of what Government is doing on the people's behalf. Looking ahead, as contemplated for instance by the Government Paperwork Elimination Act, people will conduct more and more business and other activities with the Government electronically. We cannot realize the full potential of the web until people are confident we protect their privacy when they visit our sites... Every Federal web site must include a privacy policy statement, even if the site does not collect any information that results in creating a Privacy Act record. This statement tells the visitors to your site how you handle any information you get from them. "¹
4. **PROCEDURES & GUIDELINES:**
 - (a) CNCS will post privacy policies on any agency websites used by the public.
 - (1) Policies will include:
 - Consent to collection and sharing. CNCS will clearly explain where the user may consent to the collection or sharing of information and must notify users of any available mechanism to grant consent.
 - (i) Inform visitors whenever providing requested information is voluntary.
 - (ii) Inform visitors how to grant consent for use of voluntarily-provided information.
 - (iii) Inform visitors how to grant consent to use mandatorily-provided information for other than statutorily-mandated uses or authorized routine uses under the Privacy Act.
 - CNCS will clearly explain an individual's rights under the Privacy Act if solicited information is to be maintained in a Privacy Act system of

¹ OMB Memorandum M-99-18, Privacy Policies on Federal Web Sites, June 2, 1999.

records.

- (i) Information may be provided in the body of the web privacy policy; via link to the applicable agency regulation (e.g., Privacy Act regulation and pertinent system notice); or via link to other official summary of statutory rights (such as the summary of Privacy Act rights in the FOIA/Privacy Act Reference Materials posted by the Federal Consumer Information Center at www.Firstgov.gov).
- Nature, purpose, use and sharing of information collected.
 - (i) When CNCS collects information subject to the Privacy Act, CNCS will explain what portion of the information is maintained and retrieved by name or personal identifier in a Privacy Act system of records and provide a Privacy Act Statement either:
 - (i) at the point of collection, or
 - (ii) via link to the agency's general Privacy Policy.
 - (ii) Privacy Act Statements must notify users of the authority for, and purpose and use of, the collection of information subject to the Privacy Act; whether providing the information is mandatory or voluntary; and the effects of not providing all or any part of the requested information.
 - (iii) Posted Privacy Policies must specify what information CNCS collects automatically (e.g., user's IP address, location, and time of visit) and identify the use for which it is collected (e.g., site management or security purposes).
 - Internet privacy policies should reflect that collected information may be shared and protected as necessary for authorized law enforcement activities.
 - With whom, other than law enforcement (as stated above) the information will be shared.
 - Information about management, operational and technical controls ensuring the security and confidentiality of personally identifiable records (e.g., access controls, data storage procedures, periodic testing of safeguards, etc.), and in general terms, information about any additional safeguards used to identify and prevent unauthorized attempts to access or cause harm to information and systems. (The statement should be at a level to inform the public that their information is being protected while not compromising security.)
- (2) CNCS will post (or link to) privacy policies at:
- Its principal web site.
 - Any known, major entry points to its sites.

- Any web page that collects substantial information in identifiable form.
- (3) Privacy policies must be:
- Clearly labeled and easily accessed.
 - Written in plain language.
 - Made clear and easy to understand.
- (b) CNCS will not use persistent cookies or any other means (e.g., web beacons) to track visitors' activity on the Web except for the following exceptions:
- (1) The CNCS CEO may approve the use of persistent tracking technology for a compelling need.
- When used, CNCS must post clear notice in the web privacy policy of:
 - (i) The nature of the information collected.
 - (ii) The purpose and use for the information.
 - (iii) Whether and to whom the information will be disclosed.
 - (iv) The privacy safeguards applied to the information collected.
 - CNCS must report the use of persistent tracking technologies as authorized by the CEO.
- (2) Technology that is used to facilitate a visitor's activity within a single session (e.g., a "session cookie") and does not persist over time is not subject to the prohibition on the use of tracking technology.
- (3) Customization technology (to customize a website at the visitor's request) if approved by the agency head or designee for use (see above) and where the following is posted in the Agency's Privacy Policy:
- The purpose of the tracking (i.e., customization of the site).
 - That accepting the customizing feature is voluntary.
 - That declining the feature still permits the individual to use the site.
 - The privacy safeguards in place for handling the information collected.
- (4) Agency use of password access to information that does not involve "persistent cookies" or similar technology.
- (c) CNCS will adopt machine readable technology that alerts users automatically about whether site privacy practices match their personal privacy preferences. Such technology enables users to make an informed choice about whether to conduct business with that site.
- (d) CNCS will adhere to the regulatory requirements of the Children's Online Privacy Protection Act (COPPA) when collecting information electronically from children under age 13.

- (e) CNCS will take care to ensure full adherence with stated privacy policies. For example, if a Corporation web site states that the information provided will not be available to any other entities, CNCS will ensure that no such sharing takes place.
- (f) CNCS will periodically review its web site privacy policies and practices to ensure compliance with its stated web privacy policies.

5. ROLES & RESPONSIBILITIES:

- (a) The Privacy Officer (PO) is responsible for:
 - (1) Providing guidance on development of web privacy notices.
 - (2) Verifying compliance with this policy.
- (b) Information Owners are responsible for:
 - (1) Developing and posting, or linking to, appropriate security notices
 - (2) Ensuring that posted notices are accurate and that the web site is in compliance with its notice.
 - (3) Ensuring that persistent tracking technologies are not used unless they meet the requirements for one of the exclusions specified in this policy.
 - (4) Posting machine readable policies on their web sites.
- (c) The Chief Executive Officer (CEO) is responsible for formally approving any exceptions to the ban on use of persistent tracking technology.

6. DEFINITIONS:

- (a) Cookie - Information created by a Web server and stored on a user's computer. This information lets Web sites the user visits to keep of a user's browsing patterns and preferences.
- (b) Information Privacy - The preserving of an individual's right to significantly control the handling and access of information about themselves.
- (c) Personally identifiable information (PII) - Information about an individual that identifies, links, relates, or is unique to, or describes him or her, or which can be used to distinguish or trace an individual's identity alone, or when combined with other personal or identifying information. Examples include social security number; age; corporation assigned case number; email address; home/office phone number; driver's license ID number; biometric Record; finances; education; criminal history; physical attributes; gender, etc.
- (d) Persistent Cookie - A cookie that is stored on a user's hard drive until it expires (persistent cookies are set with expiration dates) or until the user deletes the cookie.
- (e) Session cookie - Temporary cookie that is erased when you close your browser at the end of your surfing session.

(f) 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 the individual.

7. ENFORCEMENT: Violation of this policy could result in loss or limitations on use of information resources, as well as disciplinary and/or legal action, including termination of employment and referral for criminal prosecution.

8. POINT OF CONTACT: CNCS Privacy Officer

9. ATTACHMENTS: None

10. AUTHORITY:

- (a) The Privacy Act of 1974, as amended, PL 93-579, December 31, 1974
- (b) Federal Information Security Management Act of 2002 (FISMA), PL 107-347, December 17, 2002
- (c) OMB Circular A-130, Management of Federal Information Resources, Appendix III, Security of Federal Automated Information Resources, November 28, 2000.
- (d) OMB Memorandum M-03-22, OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002, September 30, 2003
- (e) OMB Memorandum M-99-18, Privacy Policies on Federal Web Sites, June 2, 1999.
- (f) OMB Memorandum M-00-13, Privacy Policies and Data Collection on Federal Web Sites, June 22, 2000.
- (g) Government Paperwork Elimination Act (GPEA), PL 105-277, Title XVII, October 21, 1998.

11. EFFECTIVE DATE: September 15, 2008

12. REVISION HISTORY: None

13. REVIEW SCHEDULE: This policy will be reviewed and updated annually.

COMPUTER DATA MATCHING

IPP-09-0808

1. **SUBJECT:** Special procedures are required when conducting computer matching programs.

2. **SCOPE:** This policy applies to electronic comparison of records which meet the following criteria:
 - Records are from two or more automated systems of records maintained by CNCS, other Federal agencies, or a contractor on the Corporation's behalf.
 - Records pertain to applicants, program beneficiaries, or providers of services to programs.
 - The purpose of the matching is to establish or verify initial or continuing eligibility for Federal benefit programs; verify compliance with the statutory or regulatory requirements of such programs; or recoup payments or delinquent debts under such Federal benefit programs.

OR

- Matches comparing records from automated Federal personnel or payroll systems of records, or such records with automated records of State and local governments.

Exclusions:

- Statistical matches with the sole purpose of aggregating data stripped of personal identifiers
 - Routine administrative matches using predominantly federal personnel records provided the purpose is not to take adverse action against personnel.
 - Law enforcement investigative matches by agencies whose principal function involves enforcement of law.
 - Internal matches using only CNCS' own records if the purpose is not to take adverse action against personnel.
 - Background investigations
3. **DESCRIPTION:** Inter-agency sharing of information about individuals can be an important tool in improving the efficiency of government programs. By sharing data, agencies can often reduce errors, improve program efficiency, identify and prevent fraud, find intended beneficiaries, evaluate program performance, and reduce information collection burden on the public.

As government increasingly moves to electronic collection and dissemination of data, under the Government Paperwork Elimination Act and other programs, opportunities to share data across agencies will likely increase. With increased focus on data sharing, agencies must pay close attention to handling responsibly their own data and

the data they share with or receive from other agencies. When information about individuals is involved, agencies must pay especially close attention to privacy interests and must incorporate measures to safeguard those interests. Prior to any data sharing, agencies must review and meet the Privacy Act requirements for computer matching, including developing a computer matching agreement and publishing notice of the proposed match in the Federal Register. Agencies must also review and meet applicable requirements under other laws, including the Paperwork Reduction Act of 1995. The Computer Matching and Privacy Protection Act (CMPPA), as amended, which amends the Privacy Act, adds certain protections for subjects of Privacy Act records whose records are used in automated matching programs and regulates the conduct of computer matching activities.

4. PROCEDURES & GUIDELINES:

- (a) Records subjects are to receive direct, constructive, and periodic notices that their records may be matched.
- (b) Notice must be published in the *Federal Register* at least 30 days prior to conducting a matching program. The notice will contain the names of participating agencies, the purpose of the match, the authority for conducting the match, categories of records and individuals covered (to include identifying the systems of records from which records will be matched), inclusive dates of the matching program, and the address for receipt of public comments or inquiries.
- (c) CNCS will obtain the written or electronic consent of individuals before sharing personal data protected by the Privacy Act, unless one of the exceptions under Section 552a(b) of the Privacy Act applies.
- (d) When receiving data from another agency under a Data Sharing program, CNCS will not re-disclose the data, except where required by law or where the redisclosure is essential to the conduct of the matching program (as allowed under the Matching Act.)
- (e) Because information shared among agencies may be used to deny, reduce, or otherwise adversely affect benefits to individuals, it is critical that CNCS have reasonable procedures to ensure the accuracy of the data shared.
 - (1) Individuals will have the right to access and to request amendment of their records, as required by the Privacy Act.
 - (2) To ensure accuracy, CNCS must also adhere to the due process requirements found in the Matching Act.
 - (3) Before CNCS takes adverse action against an individual based on the results of information produced by a matching program, it must independently verify the information unless there is a determination by the relevant Data Integrity Board, for a limited class of information, that there is a high degree of confidence that the information is accurate.
 - (4) At least 30 days before taking adverse action (unless statute or regulation states otherwise), CNCS must also provide notice to the individual of the

agency's findings and provide an opportunity to contest those findings.

- (f) Prior to the sharing of any data, CNCS will ensure that the recipient organization affords the appropriate equivalent level of security controls as maintained by CNCS. Since data security remains the responsibility of the originating agency, procedures should be agreed to in advance that provide for the monitoring over time of the effectiveness of the security controls of the recipient organization.
- (g) CNCS will analyze what data is needed for program purposes and will make every effort to ensure that it transfers only the required information.
- (h) CNCS will establish procedures to ensure compliance with redisclosure limitations.
- (i) CNCS will perform periodic self-audits to ensure compliance with the above principles
- (j) CNCS will require that the recipient agency certify on a periodic basis that it has examined practices regarding redisclosure and, if necessary, taken corrective action where improper redisclosures have occurred.
- (k) If computer matching will be used to verify program eligibility or to recover delinquent debt, CNCS will:
 - (1) Develop procedures for providing notice to the individual at the time of application, and periodically thereafter, that the information they provide may be subject to verification through matching programs, as required by the Matching Act.
 - (2) Publish a notice in the Federal Register at least 30 days before conducting the data match, describing the purpose of the match, the records and individuals covered, and other relevant information.
- (l) If CNCS receives automated records from Privacy Act systems of records of other Federal agencies or from State and local governments to be used in matching programs, CNCS is assumed to be the beneficiary of a matching program and is therefore responsible for the reporting and publishing requirements of the Act. When CNCS is the recipient agency, the component proposing the match will:
 - (1) Negotiate and draft the matching agreement.
 - (2) Publish the required notice in the *Federal Register* and report the matching program to OMB and specified Congressional Committees.
- (m) If CNCS discloses automated records from a system of records to another Federal agency or to a State or local governmental agency to be used in a matching program, CNCS will perform the following
 - (1) if the Corporation is the beneficiary of the match:
 - Negotiate and draft the matching agreement.
 - Negotiate reimbursement to the recipient agency for the costs incurred in publishing notice of the match in the *Federal Register*.

- (2) if the Corporation is not the beneficiary of the match:
 - Participate in negotiating the matching agreement.
 - Review the recipient agency's benefit/cost analysis and supplement the analysis with VA data, as appropriate.
- (3) if the recipient is not a federal agency:
 - Publish the notice in the *Federal Register* and reporting the match to OMB and Congress.
- (n) A Memorandum of Understanding (MOU) or matching agreement required for a computer matching program must contain the following:
 - (1) Purpose and legal authority
 - (2) Justification and expected results
 - (3) Description of records to be used in the match
 - (4) Procedures for notifying individuals whose records are to be matched.
 - (5) Verification methods to be used to independently verify the information obtained through the matching program
 - (6) Disposal and retention procedures.
 - (7) Security Procedures to be used in protecting the information.
 - (8) Records Usage, Duplication, and Redisclosure Restrictions.
 - (9) Records Accuracy Assessments.
 - (10) Assignment of Responsibilities for posting notices
- (o) Individuals will be afforded due process requirements when matches uncover adverse information about them.
 - (1) The Corporation will notify matching subjects of adverse information uncovered and give them an opportunity to contest such findings prior to making a final determination.
- (p) CNCS will establish a Data Integrity Board (DIB) to oversee and coordinate the Corporation's computer matching program. The board will review and approve ongoing matching program, proposed matches, pilot matches, exclusions, extensions, and renewals.
 - (1) The DIB will ensure that matching agreements and programs are in conformance with provisions of the Act as well as other relevant statutes, regulations, or guidelines, and will assess the benefits and costs of such programs. Matching agreements should remain in force only as long as necessary to accomplish the specific purpose of the match.
 - Agreements automatically expire after 18 months unless the agreement or the DIB specifies a shorter period or the DIB approves an extension not to exceed one year.

- (2) To obtain an extension, the component participating in the match must provide the DIB with certification from each party to the agreement that the program has been conducted in compliance with the agreement and that it will be conducted without change during the extension. Additional information should include the reasons that the match should be extended, including any updated benefit/cost information. GC concurrence will be obtained. The DIB must make its decision to extend a match within three months prior to the expiration date.
- (3) Renewals are treated as initial agreements and require the same documentation. Each benefit/cost analysis must contain updated information based on the actual experience of the match. All documentation must be submitted to the DIB at least two full months prior to expiration of the match.
- (4) All matching programs in which the Corporation has participated as either a source or recipient are reviewed annually. This review may include exempt matches and activities not covered by the CMPPA. The DIB determines if matches have been properly conducted, assesses the utility of the programs in terms of their benefits and costs, and reviews.

5. ROLES & RESPONSIBILITIES:

- (a) The Chief Executive Officer (CEO) is responsible for:
 - (1) Establishing a Data Integrity Board (DIB) to approve and oversee matching programs.
- (b) The Privacy Officer (PO) is responsible for:
 - (1) Providing guidance on computer matching programs
 - (2) Auditing CNCS computer matching programs for compliance with this policy.
- (c) The Privacy Act Officer will:
 - (1) Review matching agreements for legal compliance.
 - (2) Participate in the DIB.
- (d) The Chief Information Officer will:
 - (1) Participate in the DIB.
- (e) Information Owners are responsible for:
 - (1) Ensuring that any use of computer matching complies with this policy and applicable laws.
 - (2) Submitting any proposed computer matching program to the DIB and abide by its decisions and procedures.
 - (3) Developing/negotiating matching agreements
 - (4) Providing notifications to, and obtaining consent from, subjects whose data will be matched.

- (5) Developing notices for publication in the Federal Register.
 - (6) Providing due process, to subjects whose data has been matched, prior to taking adverse action.
 - (7) Ending matching programs by their agreed expiration dates.
 - (8) Validating and reporting on the status of matching programs and their compliance with the requirements of this policy.
- (f) The Office of General Counsel is responsible for posting provided SORNs to the Federal Register.

6. DEFINITIONS:

- (a) Computer Data Matching - This is the expropriation of data maintained by two or more personal data systems, in order to merge previously separate data about individuals.
- (b) Data Sharing - data matching activities or programs covered under the Computer Matching and Privacy Protection Act.
- (c) Federal Benefit Program - Any program funded or administered by the Federal government, or by any agent or State on behalf of the Federal government, that provides cash or in-kind assistance in the form of payments, grants, loans, or loan guarantees to U.S. citizens or aliens lawfully admitted for permanent residence.
- (d) Information Privacy - The preserving of an individual's right to significantly control the handling and access of information about themselves.
- (e) Matching Program. – A program that covers the actual computerized comparison and any investigative follow-up and ultimate action.
- (f) Personally identifiable information (PII) - Information about an individual that identifies, links, relates, or is unique to, or describes him or her, or which can be used to distinguish or trace an individual's identity alone, or when combined with other personal or identifying information. Examples include social security number; age; corporation assigned case number; email address; home/office phone number; driver's license ID number; biometric Record; finances; education; criminal history; physical attributes; gender, etc.

7. ENFORCEMENT: Violation of this policy could result in loss or limitations on use of information resources, as well as disciplinary and/or legal action, including termination of employment and referral for criminal prosecution.

8. POINT OF CONTACT: CNCS Privacy Officer

9. ATTACHMENTS: None

10. AUTHORITY:

- (a) The Privacy Act of 1974, as amended, PL 93-579, December 31, 1974
- (b) Federal Information Security Management Act of 2002 (FISMA), PL 107-347, December 17, 2002
- (c) OMB Circular A-130, Management of Federal Information Resources, Appendix III, Security of Federal Automated Information Resources, November 28, 2000.
- (d) OMB Memorandum M-01-05, Guidance on Inter-Agency Sharing of Personal Data - Protecting Personal Privacy, December 20, 2000
- (e) Government Paperwork Elimination Act (GPEA), PL 105-277, Title XVII, October 21, 1998.
- (f) Computer Matching and Privacy Protection Act of 1988, PL 100-503.
- (g) Computer Matching and Privacy Protection Amendments of 1990, PL 101-508.

11. EFFECTIVE DATE: September 15, 2008

12. REVISION HISTORY: None

13. REVIEW SCHEDULE: This policy will be reviewed and updated annually.

DATA EXTRACTS

IPP-10-0808

1. **SUBJECT:** All computer-readable data extracts from databases holding sensitive information must be logged and verified.
2. **SCOPE:** This policy applies to all computer-readable extracts of sensitive information, including Personally Identifiable Information (PII).
3. **DESCRIPTION:** Retrieving data from a database through a query and saving the data into a separate computer-readable entity such as another database, a spreadsheet, or a text file is a fairly common occurrence. This is often done to facilitate data analysis, reporting, transfer and other activities.

While the use of the "computer readable data extracts" can help productivity, it also exposes the data to numerous risks. Once data has been extracted, it is no longer protected by all of the security measures and procedures that protected it in the original system. Additional measures must be taken to track and protect these extracts and to ensure that they are erased when they are no longer needed. This reduces the likelihood of sensitive information being breached.

4. PROCEDURES & GUIDELINES:

- (a) All data extracts from databases that contain sensitive information must be logged.
 - (1) The logs must include the following:
 - date and time of the extract
 - name of the system/ database from which the data was extracted
 - type of extract
 - name of person who performed the extract
 - the output of the extract
 - whether the extract contains sensitive information
 - purpose of the extract
 - length of time the extract is needed
 - (2) Logs will be developed and managed in accordance with NIST Special Publication 800-53 Revision 2, Recommended Security Controls for Federal Information Systems.
- (b) CNCS will grant only authorized users access to sensitive information within each database and will provide them with only the least access necessary to perform their duties.
 - (1) Users will be restricted in the types of queries that they can perform and the

database fields (for example, social security number) that they can view and include in extracts.

- (2) Whenever possible, users will only be permitted to access sensitive information in databases through applications that tightly restrict their access to the sensitive information, instead of permitting direct database access.
- (c) Extracts should only be created when necessary and authorized.
- (d) Sensitive information, such as PII, should be scrubbed during extraction.
- (e) Data extracts containing sensitive information must be stored only on encrypted media or a secure server location (such as a locked down H or S drive on a server in a physically protected Data Center)
- (f) Sensitive data may not be extracted from a CNCS database via remote access from outside the Corporation's network.
- (g) Data extracts containing sensitive information will be protected as "sensitive information" under CNCS information security policies.
- (h) At 90 days after creation of the extract, the creator must either attest that the extract has been erased or provide a justification of why the extract is still needed.
 - (1) The erasure of extracts containing sensitive information must include sanitization in accordance with CNCS media management policies for any removable media such as CDs, diskettes, flash drives, tapes, etc.
 - (2) The Corporation will implement procedures to validate the removal of extracts.
 - (3) Extract logs will be updated to include the extract erasure date.

5. ROLES & RESPONSIBILITIES:

- (a) The Privacy Officer (PO) is responsible for:
 - (1) Providing guidance regarding the tracking of data extracts
 - (2) Reviewing extracts and logs for compliance with this policy.
- (b) Information Owners are responsible for:
 - (1) Limiting access to privacy information to the minimum necessary.
 - (2) Logging all extracts from their systems.
 - (3) Verifying the elimination of extracts.
 - (4) Scrubbing extracts to remove any unnecessary personal data.
- (c) Information Users are responsible for:
 - (1) Securely handling extracts.
 - (2) Securely disposing of extracts.
 - (3) Reporting on the disposal or continued use of the extract to the information

owner.

6. DEFINITIONS:

- (a) Data Extract - Data retrieved from a database through a query and saved into a separate computer-readable entity such as another database, a spreadsheet, or a text file
- (b) Personally Identifiable Information (PII) – Information about an individual that identifies, links, relates, or is unique to, or describes him or her, or which can be used to distinguish or trace an individual’s identity alone, or when combined with other personal or identifying information. Examples include social security number; age; corporation assigned case number; email address; home/office phone number; driver’s license ID number; biometric Record; finances; education; criminal history; physical attributes; gender, etc.

7. ENFORCEMENT: Violation of this policy could result in loss or limitations on use of information resources, as well as disciplinary and/or legal action, including termination of employment and referral for criminal prosecution.

8. POINT OF CONTACT: CNCS Privacy Officer

9. ATTACHMENTS: None

10. AUTHORITY:

- (a) The Privacy Act of 1974, as amended, PL 93-579, December 31, 1974
- (b) Federal Information Security Management Act of 2002 (FISMA), PL 107-347, December 17, 2002
- (c) OMB Circular A-130, Management of Federal Information Resources, Appendix III, Security of Federal Automated Information Resources, November 28, 2000.
- (d) OMB Memorandum M-06-16, Protection of Sensitive Agency Information, June 23, 2006
- (e) OMB Memorandum M-07-16, Safeguarding Against and Responding to the Breach of Personally Identifiable Information, May 22, 2007.
- (f) OMB Memorandum M-07-16 Data Extract Frequently Asked Questions (FAQ).
- (g) NIST Special Publication (SP) 800-53 Revision 2, Recommended Security Controls for Federal Information Systems

(h) NIST SP 800-92, Guide to Computer Security Log Management.

11. EFFECTIVE DATE: September 15, 2008

12. REVISION HISTORY: None

13. REVIEW SCHEDULE: This policy will be reviewed and updated annually.



**Corporation for National & Community Service
Office of Information Technology**

**Information Privacy
Program Handbook**

August 2008

TABLE OF CONTENTS

1. INTRODUCTION	1
2. ROLES & RESPONSIBILITIES	8
3. TRAINING & AWARENESS	12
4. COMPLYING WITH POLICIES	14
5. PRIVACY INCIDENTS	18
6. COLLECTING PRIVACY DATA	20
7. PROTECTING PRIVACY DATA	21
8. TRACKING PRIVACY DATA	24
9. SYSTEM OF RECORDS (SOR)	26
10. PRIVACY IMPACT ASSESSMENTS	32
11. DATA EXTRACTS	35
12. WEB SITE PRIVACY	37
13. COMPUTER DATA MATCHING	42
14. PROGRAM GOVERNANCE	46
APPENDIX A: INFORMATION PRIVACY GLOSSARY	48
APPENDIX B: ACRONYMS AND ABBREVIATIONS	50

1. INTRODUCTION

The Corporation for National and Community Service (CNCS) requires that individuals provide information about their lives, financial status, health status, and other activities in support of the Corporation's mission. This information may be required to support hiring actions for employees or to qualify for participation in various contract, grant, and volunteer activities. Individuals provide this information with the expectation that the Corporation will exercise due care to protect the information entrusted to them from unauthorized access and will use that information only for the purpose for which it was provided.

Recognizing the need for individuals to continue to voluntarily provide the government with their personal information, and the responsibility of the Government to protect this information, Congress and the Office of Management and Budget (OMB) enacted laws and regulations requiring that federal agencies establish Privacy Programs to monitor the collection of personal information and to protect that information once it has been collected.

In the past few years, privacy concerns have significantly increased in importance and are now continuing items of concern for senior government managers. Three factors are driving the concern for information privacy:



- The increasing number and impact of information compromises has raised public awareness that a single security failure can adversely impact millions of individuals. Further, these impacts generally require the affected individuals to take action to protect themselves, as the organization where the breach occurred can do nothing to restore information confidentiality once it has been compromised.
- The use of the Internet and other advanced technologies have provided information processing efficiencies, allowing data to be shared globally with ever decreasing timeframes. These same efficiencies, however, greatly expand the scope and damage that can be done by a single information compromise.
- Federal agencies maintain large databases of information relating to individuals. For example, the Corporation maintains information regarding thousands of individuals who have participated in or requested participation in its volunteer and internship programs. Individuals have raised concerns that this information can be too easily shared and used for purposes other than those for which it was intended.

Broadly stated, the purpose of federal privacy requirements is to balance the government's need to maintain information about individuals with the rights of individuals to be protected against unwarranted invasions of their privacy stemming from federal agencies' collection, maintenance, use, and disclosure of personal information about them.

OMB guidance regarding implementation of the E-Government Act requires that federal agencies establish and maintain an Information Privacy Program. OMB has issued several memoranda that provide guidance and requirements related to the management of Personally Identifiable Information (PII).

1.1 What is "Information Privacy"?



“Privacy is the claim of individuals, groups or institutions to determine for themselves when, how, and to what extent information about them is communicated to others”¹. Individuals have a right against unsanctioned invasion of privacy by the government, corporations or individuals. However, privacy is not an absolute. “Each individual is continually engaged in a personal adjustment process in which he balances the desire for privacy with the desire for disclosure and communication.”²

Information privacy is the aspect of privacy that deals with an individual's expectations and rights regarding data about him or herself. Privacy concerns exist wherever data is uniquely identifiable to a specific person or persons, whether electronic or not. Concerns about data privacy arise in many areas, from the confidentiality of data to how it is used.

In order for an individual to make informed decisions about the privacy of his or her information, they must be given notice about the information that is collected about them, what it will be used for, who will have access to it, what choices they have regarding its collection and use, and what their rights are under the law.

When the information collected is used to make decisions about the individual, either directly or indirectly, such as when it affects credit worthiness, is used to make hiring decisions, or determines eligibility for a government program, issues also arise regarding the accuracy of the information. Individuals must have the right to access and request corrections to their data in order to ensure that they are being treated fairly.

CNCS' Information Privacy Program must address the whole range of these issues to ensure that individuals maintain the right to control the access and use of their data as well as be assured that the data about them used by the government is correct. This includes not only protecting the confidentiality of personal information, but also ensuring that the information is collected and maintained in accordance with informed decisions made by the data subject.

1.2 What is covered under Information Privacy?

Most individuals recognize that certain data (e.g., Social Security Number) deserves special protection because of the harm or damage that could result from a data compromise. Identifying PII, however, is not always that easy. As defined in the Privacy Act and the E-Government Act, PII may be any information that can explicitly or implicitly identify a single individual. Thus, while it is obvious that a Social Security Number meets this definition, it may not be apparent that telephone numbers, computer logon IDs, badge numbers, and e-mail addresses can also be individual identifiers. Privacy information can be any information that directly identifies an individual (e.g., name, address, social security number or other identifying number or code, telephone number, email address, etc.) or any information by which an agency intends to identify specific individuals in conjunction with other data elements, i.e., indirect identification. These data elements may include a combination of gender, race, birth date, geographic indicator, and other descriptors. Health, financial, personal affiliations, and lifestyle information are other examples of information that should be protected under privacy regulations.

¹ Alan Westin: Privacy & Freedom, 1967

² Alan Westin, 1967

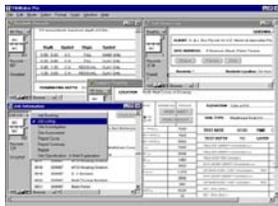
**1.2.1
 Combining
 information**

The combination of different pieces of information that might not individually require privacy protection may result in a record that does require privacy protection. For example, a phone number or an address on its own may not be private, but when combined with name and other information, it must then be protected. Each combination of information must be assessed to determine the risk posed by the set as a whole.

**1.2.2
 The source of the
 information is
 important**

The source of the information also matters in determining the privacy rules for the information. For example, the use and protection of ANY information collected under a Privacy Act System of Records (discussed in section 9) is governed by the System of Records Notice for that system. Likewise, when collecting information via the web, you must use and protect the information in accordance with the posted privacy notice you provided when you collected the information. When using data provided by another agency or organization, you are bound by the agreements put in place for that data transfer. The promises that the Corporation makes in notices and agreements are binding, and must be fulfilled regardless of the nature of the actual information.

**1.2.3
 What privacy
 information does
 CNCS have?**



CNCS information that must be protected from an Information Privacy perspective includes, but is not limited to, the following:

- **Member/Grantee Information** is collected and used to screen applicants, manage grants, operate programs, and carry out the Corporation's mission. Examples include: social security numbers, contact information, background investigations, and medical data.
- **Personnel Information** is necessary for CNCS to administer human capital programs, including compensation and benefits. Examples include payroll information; benefits information; retirement information; time and attendance information; and program information (e.g., staffing, employee relations, etc.).
- **Financial Information** is essential for CNCS to carry out its financial functions and activities. Examples include accounts payable information, grant information, VISTA payroll information, and travel documents.
- **Program and Legal Information** is essential for CNCS to carry out its programmatic and legal functions and activities and to protect the U.S. government and the legal and financial rights of CNCS' customers. Examples include client information; grant documentation; working documents; and FOIA information.

**1.3
 Why is Information
 Privacy important?**

The purpose of federal privacy requirements is to balance the government's need to maintain information about individuals with the rights of individuals to be protected against unwarranted invasions of their privacy stemming from federal agencies' collection, maintenance, use, and disclosure of personal information about them. The Privacy Act of 1974 (5 U.S.C. § 552a) was enacted because Congress was concerned with curbing the illegal surveillance and investigation of individuals by federal agencies; it was also concerned with potential abuses presented by the

1.4

What are the harms that could occur to individuals due to our handling of their information?



government's increasing use of computers to store and retrieve personal data by means of a universal identifier – such as an individual's social security number.

CNCS collects personal information about employees, members, grantees, and other individuals for a variety of authorized purposes to deliver efficient and effective services. In order to fulfill its mission, the Corporation must protect this information. "It is hard to put a value on trust, but it is easily one of our most precious assets. We could not function without it and the truth is it could be lost in an instant. To earn and maintain the trust of our customers and the general public we must continuously safeguard all private data we hold. Doing this helps us comply with laws, regulations and policies, and helps us avoid costly lawsuits, fines and negative publicity."³

Invasion of Privacy

Individuals may not want personal information about themselves, such as their religion, sexual orientation, political affiliations, or personal activities, to be revealed to others without their permission. Disclosure of this information could lead to discrimination, personal embarrassment, or damage to one's professional reputation.

Additionally, information about a person's financial transactions can reveal a lot about that person's history, such as places they have visited, whom they have had contact with, products they use, their activities and habits, or medications they have used.

Medical records are another area of sensitive information that a person may not want revealed to others. "This may be because they have concern that it might affect their insurance coverage or employment. Or it may be because they would not wish for others to know about medical or psychological conditions or treatment which would be embarrassing. Revealing medical data could also reveal other details about one's personal life (such as about one's sexual activity for example)."⁴

Invasion of Privacy may occur in a variety of ways, including (but not limited to):

- Corporation staff snooping at someone's file out of personal curiosity.
- Accidental posting or exposure of information on the web or other public system.
- Loss of equipment or media containing private information.
- Intentionally hacking into the system or performing dumpster diving to snoop on someone else's information.
- Accessing the system to obtain information for blackmail or extortion purposes.
- Intentional exposure of information to cause embarrassment or harm.
- Unsecure disposal of paper documents, which either accidentally exposes information or which can be exploited by dumpster divers.
- Release or sale of information, without the individual's permission, to businesses that may spam or telemarket the individual.

³ Inspired eLearning, Privacy 101

⁴ Wikipedia, "Privacy"

Identity Theft

If criminals gain access to information such as a person's account or credit card numbers, that person could become the victim of fraud or identity theft.

“Identity theft—the misuse of another individual’s personal information to commit fraud—can happen in a variety of ways, but the basic elements are the same. Criminals first gather personal information, either through low-tech methods such as stealing mail or workplace records, or “dumpster diving,” or through complex and high-tech frauds such as hacking and the use of malicious computer code. These data thieves then sell the information or use it themselves to open new credit accounts, take over existing accounts, obtain government benefits and services, or even evade law enforcement by using a new identity. Often, individuals learn that they have become victims of identity theft only after being denied credit or employment, or when a debt collector seeks payment for a debt the victim did not incur.”⁵



Identity theft not only causes financial loss, it also affects a person's credit rating which can have widespread impact on their lives, from qualification for financial transactions to employment screenings. It also exacts an emotional toll on the individual and their family, who might have to fight for years to get the situation resolved.

Identity Theft is a threat from both insiders and outsiders. “According to law enforcement agencies, identity thieves often have no prior criminal background and sometimes have pre-existing relationships with the victims. Indeed, identity thieves have been known to prey on people they know, including coworkers, senior citizens for whom they are serving as caretakers, and even family members... Occasionally, small clusters of individuals with no significant criminal records work together in a loosely knit fashion to obtain personal information and even to create false or fraudulent documents.”⁶

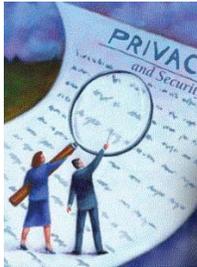
Unfair Treatment by the Government

There are additional concerns when information about private citizens is collected by the government. This is particularly an issue when the government uses this data to make decisions, such as awarding benefits or taking criminal action. The Privacy Act was enacted to protect citizens from Government keeping secret databases of information about them. The Act requires citizens to be notified when their information is collected, informed about its use, and provided access to view and correct the information so that decisions are correctly made. Failing to do so may result in unfair treatment of individuals by the government.

⁵ Identity Theft Task Force, *Combating Identity Theft: A Strategic Plan*, April 2007

⁶ U.S. Attorney’s Office, Southern District of Florida, Press Release (July 19, 2006), available at <http://www.usdoj.gov/usao/fls/PressReleases/060719-01.html>

1.5 What is the Privacy Act?



For more information on the Privacy Act, visit www.usdoj.gov/oip/privstat.htm

1.6 What are the other key laws and mandates guiding CNCS Privacy requirements?



The Privacy Act establishes safeguards for the protection of records the Government collects and keeps on individuals. The Privacy Act provides the Government with a framework in which to conduct its day-to-day business when that business requires the collection or use of information about individuals. Specifically, it requires that the Government:

- Maintain no secret files on individuals.
- Inform individuals at the time it is collecting information about them, why this information is needed, and how it will be used.
- Assure that personal information is used only for the reasons given, or seek the person's permission when another purpose for its use is considered necessary or desirable.
- Allow individuals to see the records kept on them, and provide individuals with the opportunity to correct inaccuracies in their records.

The Privacy Act binds Federal agencies to a "code of fair information practices." The code sets standards which each Federal agency must meet as it collects, maintains, and uses information.

Specifically, the Privacy Act applies to Agency records that:

- Contain information on individuals, and
- Are filed so that the records are retrieved by the person's name or some other personal identifier, such as a social security number.

The Privacy Act applies to personal information stored on computers as well as in paper files.

Laws and other federal guidance applicable to privacy include:

- The Computer Matching and Privacy Protection Act of 1988
- Computer Matching and Privacy Protection Amendments of 1990
- The Government Paperwork Reduction Act of 1995 (44 U.S.C. § 101 note) and the Information Technology Management Reform Act of 1996 (also known as Clinger-Cohen Act)
- Federal Information Security Management Act of 2002 (FISMA)
- Office of Management and Budget (OMB) Circular No. A-130, Transmittal No. 3, Appendix I, "Federal Agency Responsibilities for Maintaining Records About Individuals"
- OMB Circular A-123, "Management Accountability and Controls"
- Freedom of Information Act of 1996 (FOIA)
- Section 208 of the E-Government Act of 2002 (44 U.S.C. § 3501 note)
- Office of Management and Budget (OMB) Memoranda
- National Institute of Standards and Technology (NIST) Guidance
- Health Insurance Portability and Accountability Act of 1996 (HIPAA)
- 5 CFR part 293, "Personnel Records"

- Gramm Leach Bliley Act

Additionally, there are many state and local laws applicable to information privacy.

1.6.1 International Laws

Many countries have much more stringent Privacy laws than the United States, and privacy is often seen as a basic human right. If you collect or use information from persons in any other country or persons who are foreign citizens, then you must make sure you are in compliance with the relevant laws. Please contact the Office of General Counsel for assistance with this.

1.7 What is the Information Privacy Program (IPP)?

The CNCS Information Privacy Program (IPP) is a comprehensive set of initiatives intended to ensure that CNCS protects the information privacy rights of individuals about whom we collect data and is compliant with all federal regulations and other applicable laws.

The program includes policies and procedures that specify how to securely and legally use privacy protected information at CNCS. Also included is a comprehensive set of activities to promote privacy awareness and educate everyone at CNCS on their information privacy responsibilities.

1.8 What is included in the program and how is the program structured?



The core of the program is a set of information privacy policies, based on legal requirements, federal government standards, and CNCS management objectives, that specify the “rules” for using and protecting privacy information. Each policy discusses a specific privacy topic. The policies incorporate requirements and guidelines, roles and responsibilities, penalties for violations, the reason for each policy, and other important information pertaining to the particular privacy topic.

To make it easier for you to understand the information privacy requirements, and your privacy responsibilities, we have developed this Handbook. The Handbook serves as your primary reference for understanding and meeting your information privacy responsibilities.

Additionally, information privacy training is provided, and required, for all CNCS personnel, to make sure that everyone understands CNCS privacy policies and maintains awareness of privacy issues.

1.9 Where Do I Get More Information?

Copies of the CNCS information privacy policies, as well as additional privacy-related information will be posted on the intranet

1.10 Who can I contact if I have questions?

If you have any questions about information privacy, please contact the CNCS Privacy Officer, Laurie Young, at 202-606-6662.



2. ROLES & RESPONSIBILITIES

Your information privacy responsibilities are based on your role in the Corporation. This section specifies the roles defined in the Information Privacy Program and their associated responsibilities. It is imperative that you understand what your role(s) and responsibilities are.

2.1 Who is responsible for Information Privacy at CNCS?

EVERYONE who handles any privacy information at CNCS shares in the responsibility to protect that information and to use it appropriately. This includes employees, contractors, interns, members, volunteers, temporary workers, etc.

2.2 What are your specific roles and responsibilities regarding privacy?

For the purpose of assigning security and privacy responsibilities, some general roles have been defined. Each policy specifies the particular responsibilities that are assigned to each of these roles as applicable.

Individuals may serve in multiple roles for different aspects of their jobs. For example, a Program Director may serve as an Information Owner for a particular system, as a Supervisor for the employees in his/her department, and as a User of information. All of these roles have information privacy responsibilities.

The roles defined are as follows:

2.2.1 Information Users

Information Users are individuals who use or have access to CNCS' information, including employees, interns, temporary workers, contractors, etc. All individuals who use CNCS information are responsible for protecting the information entrusted to them and complying with CNCS information privacy policies and procedures.

Information User responsibilities include:

- Adhering to all CNCS information privacy policies.
- Not disclosing any personal information contained in any system of records except as authorized. Personnel willfully making such a disclosure when knowing that disclosure is prohibited are subject to possible criminal penalties and/or administrative sanctions.
- Reporting any unauthorized disclosures of personal information from a system of records or the maintenance of any system of records that are not authorized to your local Privacy Act Officer or to your supervisor.



2.2.2 Supervisors

Supervisors are employees who have some kind of supervisory relationship over other staff. This can include managers, COTRs, visitor escorts, etc. Supervisors ensure that their staff understands their privacy responsibilities, comply with CNCS policies, and maintain privacy awareness.



2.2.3 Information Owners



Supervisors are responsible for:

- Ensuring that their staff have the necessary training to effectively comply with CNCS privacy policies and procedures.
- Monitoring staff performance to ensure compliance with CNCS privacy policies.
- Helping to enforce policies.
- Serving as a good example for their employees to follow.
- Providing privacy guidance to their staff.
- Reporting potential violations of privacy policy or potential compromise of PII to the Privacy Officer.
- Implementing remedial actions when their staff violates privacy policies.

Information Owners are the individuals ultimately responsible for specific information resources (including data collections). Information Owners are usually managers or directors who own information on behalf of their departments. It is the information owner's responsibility to ensure that the resources they own are compliant with CNCS information privacy policies and procedures. Information Owners must be federal staff.

Information Owners are responsible for:

- Identifying PII included in the system for which they are responsible.
- Ensuring that the use of PII is restricted to the minimum necessary to complete program objectives.
- Ensuring that there is authorization and a business need for collection of the identified PII in the system for which they are responsible.
- Determining whether the system for which they are responsible constitutes a "System of Records" as defined in the Privacy Act and if so, ensures that a System of Records Notice (SORN) covering their system is in place.
- Reviewing biennially each SORN to ensure that it accurately describes the system of records.
- Making a determination as to whether a PIA is required and submit that determination to the Privacy Officer (PO).
- Ensuring that a PIA is completed on each system as required.
- Ensuring that privacy statements are appropriately posted, comply with CNCS policy, and have been reviewed and approved by the PO and General Counsel.
- Ensuring data collection forms include privacy notification statements.
- Ensuring that systems directed at children incorporate a method for verifiable parent consent for collection of information for children under the age of 13.
- Monitoring contractor compliance with the Privacy Act.

2.3 Are there specific individuals who have a special role in privacy at CNCS?



- Ensuring that users of the system are trained on the specific handling requirements and safeguards.
- Ensuring that a log is maintained of access and amendments to records, and disclosures of the records.
- Ensuring that CNCS websites do not employ persistent tracking technologies.
- Implementing, testing, and maintaining machine-readable privacy policies on existing websites and websites in development.
- Ensuring that a privacy notice has been developed and is accessible as a link on each CNCS webpage.
- Ensuring that official files on individuals that are retrieved by name or other personal identifier are not maintained without first ensuring that a Privacy Act system of records notice has been published in the Federal Register. Any official, who willfully maintains a system of records without meeting the publication requirements of the Act, is subject to possible criminal penalties and/or administrative sanctions.
- Reporting potential violations of privacy policy or potential compromise of PII to the Privacy Officer.

In addition to the general roles described above, there are individuals at CNCS who have been assigned additional responsibilities regarding the safeguarding of sensitive personal information. These include:

- The Chief Executive Officer (CEO) is responsible for ensuring that the information privacy policies, procedures, and practices of the Corporation are adequate. The CEO also designates a Senior Agency Official for Privacy (SAOP).
- Senior Agency Official for Privacy (SAOP) - The SAOP has overall responsibility and accountability for ensuring the Corporation's implementation of information privacy protections, including full compliance with federal laws, regulations, and policies relating to information privacy.
- The Privacy Officer is responsible for developing and operating the Privacy program, and ensuring privacy compliance across the organization. The Privacy Officer is responsible for developing privacy policies and guidance and ensuring their dissemination and implementation throughout the Corporation.
- The Privacy Act Officer - The Office of the General Counsel (OGC) assigns one of their staff to serve as the Freedom of Information Act (FOIA) Officer and the Privacy Act Officer to adjudicate records requests. The Privacy Act Officer is responsible for reviewing CNCS Privacy Act System of Records Notices (SORN) prior to publication, advising the CEO and the Senior Agency Official for Privacy on matters involving interpretation of the provisions of the Privacy Act, and supporting the Senior Agency Official for Privacy in annual reporting on the effectiveness of the agency privacy program.
- The Privacy Advocate ensures that privacy is considered within the Office of

Human Capital's (OHC) programs and business processes. The Privacy Advocate reviews and evaluates activities related to personally identifiable information collected and maintained by OHC.

- The Chief Information Security Officer (CISO) ensures the confidentiality, integrity and availability of information and information systems through formal policies, awareness training, monitoring compliance and access controls. The CISO works with the Privacy Officer to ensure the integration and effectiveness of the security and privacy programs.
- The Chief Human Capital Officer (CHCO) is responsible for the security and privacy of the Corporation's personnel records. The CHCO assigns one of his staff to serve as the Privacy Advocate.
- The Chief Information Officer (CIO) oversees the programs of the Office of Information Technology. The CIO promotes a coordinated, interoperable, secure and shared corporate IT infrastructure. Additionally, the CIO serves as a corporate-wide resource for major policy, program, or operational initiatives.
- Procurement Services is responsible for ensuring that all agency contracts and procurements are compliant with the agency's information privacy policy and contain appropriate information privacy clauses.

As of April 2008, the following individuals are assigned to these roles.

Role	Individual Assigned
Chief Executive Officer (CEO)	David Eisner
Chief Information Officer (CIO)	Alan Friend (Acting)
Chief Information Security Officer (CISO)	Juliette Sheppard
Privacy Officer	Laurie Young
Senior Agency Official for Privacy (SAOP)	Alan Friend (Acting)
Privacy Act Officer	Austin Holland
Privacy Advocate	Norm Franklin
Chief Human Capital Officer (CHCO)	Ray Limon
Director of Procurement Services	Roderick Gaither



3.1 Understanding and accepting your Information Privacy responsibilities

3.1.1 Reviewing and understanding CNCS' Information Privacy Policies



3.1.2 Completing Information Privacy training

3. TRAINING & AWARENESS

Information Privacy is a continuous effort and "state of mind". This is achieved by reinforcing concerns and appropriate behaviors on an ongoing basis. Effective information privacy is achieved when it becomes part of everyone's thinking with regard to daily operations and assignments. Therefore, Privacy Training and Awareness is crucial to the effectiveness of the Information Privacy Program.

An important aspect of CNCS' Information Privacy Program (IPP) is ensuring that everyone understands and accepts their individual privacy responsibilities. Only by making everyone aware of their privacy responsibilities and teaching them correct practices can CNCS reduce the level of risk to privacy information.

Many components of CNCS' IPP are aimed at improving staff awareness of the need to protect privacy information, and building individual accountability. Information privacy policies and standards cannot be effective unless everyone, regardless of their level in the organization, is aware of the importance of information privacy, understands CNCS procedures, and performs required practices.

Whether you are an employee, an intern, a temporary worker, a contractor, a member, a volunteer, or any other type of staff, information privacy is your personal responsibility, and you serve a critical role in protecting the information to which you have been granted access. As such, you are responsible for familiarizing yourself with, and abiding by, the policies outlined in this Handbook.

This Handbook provides information and instructions on:

- Fulfilling your privacy responsibilities.
- Privacy considerations.
- Policies and procedures you must follow when handling privacy information.

You should also take the opportunity to review the detailed Information Privacy Policies (IPPs).

It is your responsibility to make sure you read and understand these policies and procedures. If you have questions, please ask your supervisor or the Privacy Officer for clarification.

Every federal agency must provide mandatory periodic information privacy training to all employees involved in the use or management of privacy information. A Privacy Training and Awareness program is crucial to the safeguarding of CNCS privacy information. For these reasons, all employees, including interns, as well as contractors, and other personnel who have internal access to CNCS information resources, must complete CNCS' information privacy training program. This training consists of the following activities:

For more information on Information privacy Training, see IPP-02, *Privacy Training & Awareness*.

3.1.3 Completing the "Privacy Rules of Behavior" Agreement

3.1.4 Maintaining Privacy Awareness



- Information privacy training incorporated into the new hire and new contractor orientation processes.
- Annual information privacy refresher training.
- Personnel with additional privacy responsibilities, such as Information Owners, must complete additional privacy training specific to their responsibilities.

Information privacy training may be in the form of classroom, one-on-one, computer-based, or other format, as determined by the PO.

All CNCS employees, interns, contractors, and other personnel, must acknowledge and agree to comply with CNCS' information privacy policies and procedures. The "Privacy Rules of Behavior" is to be signed by each staff member (employee, contractor, etc.) upon completion of information privacy orientation training and before being granted access to PII.

The form is available for download from the security page on the intranet.

One of CNCS' information privacy program goals is to help staff maintain privacy awareness on an ongoing basis. Information privacy is not a one-time event, but a continuous effort and a "state of mind." This is achieved by reinforcing appropriate behaviors and mindset on a continuous basis. Effective information privacy is achieved when it becomes part of everyone's thinking with regard to daily operations and assignments.

CNCS' privacy awareness program sets the stage by changing organizational attitudes to realize the importance of privacy and the adverse consequences of noncompliance. It also reminds users of the procedures that must be followed. Hopefully, awareness will stimulate and motivate all CNCS staff to care about privacy and remind everyone of important privacy practices.

The PO will periodically issue information notices to CNCS employees to remind them of basic privacy practices (*e.g.*, protecting your passwords).

It is your responsibility to exercise privacy awareness at all times when performing your CNCS duties, and to take an active part in protecting privacy information.



4. COMPLYING WITH POLICIES

Everyone who handles privacy information shares a responsibility to the individuals about whom the data applies. This includes not just securing the data, but also ensuring that the individual's rights are upheld through the process from collection to disposal. By complying with Corporation privacy policies and fulfilling your privacy responsibilities, you ensure that the Corporation provides fair treatment to members, volunteers, employees, and anyone else about whom we collect, maintain, or use information. Additionally, there are federal and state laws under which you could face criminal or civil penalties for failing to uphold individuals' privacy rights.

4.1 What are the rules?



For more information, please see the privacy policies.

You are required to protect any privacy information, including both electronic and paper records, in your custody from unauthorized disclosure, modification or destruction so that the security and confidentiality of the information is preserved.

Use and disclose information only as authorized, and as permitted by posted privacy policies and systems of record notices.

Collect only the minimum PII necessary, and securely dispose of it when no longer needed.

Complete all requested privacy training and awareness activities on time, and sign an agreement to comply with CNCS information privacy policies (Privacy Rules of Behavior).

Comply with all laws, federal requirements, and CNCS policies and procedures regarding handling of privacy data.

Report any suspected unauthorized disclosures of PII in accordance with CNCS Information Security incident reporting procedures, and fully cooperate with investigations.

4.2 What happens if CNCS Information Privacy policies are violated?

If anyone is found to be knowingly, willfully, or negligently in violation of any CNCS information privacy policy or any of the provisions in this Handbook, they will be subject to administrative or disciplinary actions, including, but not limited to:

- Loss or limitations on use of information resources,
- Disciplinary action, from warning to termination of employment, and/or
- Referral for criminal prosecution.

Additionally, the Privacy Act specifies the following consequences for violations of the Act:

- Any official who willfully maintains a Privacy Act system of records without meeting the publication requirements is subject to possible



4.2.1 What is an Information Privacy violation?

criminal penalties or administrative sanctions, or both.

- Any person who knowingly and willfully requests or obtains any Privacy Act record concerning an individual from an agency under false pretenses shall be guilty of a misdemeanor and fined not more than \$5,000.
- Any employee with possession of, or access to PII who willfully discloses the material in any manner to any person or agency not entitled to receive it, may be guilty of a misdemeanor and fined not more than \$5,000.
- Employees may be subject to written reprimand, suspension, or removal under situations including, but not limited to:
 - Failing to implement and maintain required information security controls for the protection of PII, regardless of whether such action results in the loss of control or unauthorized disclosure of PII.
 - Failing to report any known or suspected loss of control over, or unauthorized disclosure of, PII.
 - For managers, failing to adequately instruct, train, or supervise employees in their responsibilities.

An information privacy violation is any breach of CNCS information privacy policies, procedures or guidelines, whether or not privacy information is actually compromised. Information privacy violations may occur knowingly, willfully, or through negligence. Any action or a failure to adhere to CNCS information privacy policies is considered a privacy violation.

Examples of information privacy violations include, but are not limited to:

- Failure to comply with CNCS information privacy policies and practices, including those outlined in this Handbook.
- Failure to perform your information privacy responsibilities
- Violation of any Federal or state administrative, legislative, judicial or criminal laws or procedures regarding privacy.
- Assisting staff, contractors, or any external entities or individuals in performing any information privacy offense.

4.2.2 What determines the severity of a violation?

The significance of an information privacy violation does not depend only on whether information was actually compromised. It also depends on the intentions and attitudes of the individual who commits the violation. Access to CNCS information is a privilege that may be changed or revoked at the discretion of management. Ability and willingness to follow the rules for protection of CNCS information is a prerequisite for maintaining access to that data.

4.2.3 How does CNCS handle a violation?

After receiving notification of a possible violation, the Privacy Officer (PO) may initiate an inquiry to determine whether privacy information has been compromised. Based on the findings, the PO may refer the matter to the Office of the Inspector General for further action. The specific circumstances of the violation determine what sanctions, remedies or penalties CNCS will pursue.

4.3 What if I can't comply with a policy?

CNCS information privacy policies have been developed in accordance with federal guidance and will be implemented consistently to ensure effectiveness. However, there are occasional circumstances in which it is not completely feasible or in the best interests of the Corporation to comply with a particular policy provision or to do so within a particular timeframe. In such cases, there is a formal waiver process to evaluate and approve exceptions to the policies. These waivers will be granted in rare situations under specific circumstances and will be based on an analysis of risk. Additionally, please note that some privacy provisions cannot be legally waived.

4.3.1 When do I need a waiver?

In general, failure to comply with a policy will result in some sort of disciplinary action. In cases where you or a system that you own cannot comply with a policy or if complying with the policy would not be prudent and in the best interests of the government, you need to obtain a waiver to avoid the consequences of non-compliance. However, waivers are not intended to be used to pardon offenses that have already been committed. Requests are to be submitted as far in advance as possible.

4.3.2 How do I request a waiver?

A waiver request may be submitted to the PO using the CNCS waiver request form. If the waiver is for a system, the request should be submitted by the system owner.

The waiver request must provide:

- A legitimate justifiable reason for waiving a privacy requirement.
- The specific scope and circumstances of the waiver (e.g., period of waiver, specific resources or persons for which the requirement is waived, etc.)
- An understanding of the risks involved
- A recommendation for compensating control(s) to mitigate the risk resulting from the waiver.

4.3.3 What is the waiver approval process?

The PO, in consultation with applicable personnel (e.g., the CISO, CIO, CFO, General Counsel, etc.) will evaluate and respond to waiver requests. In the specific cases prescribed by federal guidance that require signature of the agency head for a particular waiver situation, the request will be escalated to the CEO.

Waiver requests will be evaluated based on the following criteria:

- Waivers will only be granted if it is within the Corporation's right to do so. Waivers cannot be approved that would violate legal requirements.
- An assessment of whether the reason for the waiver is truly accurate and justified, and whether there are alternatives for meeting the requirement that could be pursued.
- An analysis of the risks and proposed mitigation strategy

4.3.4 Do waivers expire?

Each waiver is approved for a specific period of time. Upon expiration of the granted waiver period, the waiver can be submitted for renewal if it is still needed. If a waiver is not renewed prior to the expiration of the period specified in the waiver, it will cease to be in effect at the end of the period.

If you or your system simply need additional time to implement a policy, your waiver request should include the amount of time you need to achieve compliance.

Waivers granting exceptions to policies (rather than delays) will be good for a period of 1-3 years depending on the nature of the exemption. This will allow for periodic re-evaluation of the need for the waiver.





5. PRIVACY INCIDENTS

Incident management is crucial to the Privacy program. The adverse impact from a compromise of PII can significantly increase the longer a compromise remains. Potential privacy incidents must be reported promptly and mitigating actions must be effected as quickly as possible. The Corporation must be able to respond to privacy-related incidents in a manner that protects its own information and helps to protect the information of others that might be affected by the incident.

5.1 Reporting Information Privacy incidents

You must immediately report any suspected information privacy incidents so that CNCS may respond in a timely manner to correctly handle the incident, stop the problem from escalating, and minimize the impact on affected individuals. Your cooperation and participation in reporting privacy incidents is vital to CNCS' maintaining the privacy of its information resources. It is important that all information users maintain vigilance regarding information privacy, and immediately report any suspected incidents in order to minimize potential damage to CNCS.

5.2 What is an "Information Privacy Incident?"

A privacy incident is any occurrence that actually or potentially jeopardizes the confidentiality of privacy information, or violates privacy policies, procedures, or laws. A privacy breach is not limited to intrusion or accidental exposure of the data, but also includes any collection, use, disclosure, or retention of data that is not in accordance with established notices, agreements, and laws.

Examples of potential privacy incidents include:

- Loss/theft of a device containing privacy information.
- Unauthorized viewing of privacy information by staff.
- Accidental publication or distribution of privacy information
- Hacker breaching a system containing privacy information.
- Noncompliance with privacy policies.
- Failure to perform your privacy responsibilities.
- Collection of PII without a published notice
- Information disclosure that isn't compliant with the posted privacy notice.

5.3 How do you report an Information Privacy Incident?

You must report suspected incidents to the Privacy Officer, CISO, the OIT Help Desk, the Information Owner or your supervisor as quickly as possible. You may report incidents either verbally or in writing.

If you receive incident reports from staff, you must immediately pass them on to the Privacy Officer. The Corporation is required to report any suspected incidents involving PII to US-CERT within one hour of discovery, so your timely reporting of the incident to us is essential.

If the incident involves loss or theft of any Corporation equipment, you must

For more information, see IPP- 04, *Privacy Incident Management*.

5.4 How does the Corporation respond to reported incidents?



complete a "Missing IT Asset Impact Analysis" form (available on the information security page on the intranet)

You may also be requested to document relevant information or assist with resolution of the incident. Your full cooperation in resolving the incident is required.

The Corporation follows the CNCS Information Security Incident Response Procedures for all incidents. If an incident involves privacy information, the Corporation invokes the Privacy Incident Response Team (PIRT) which is responsible for responding to the loss of personal information. The PIRT performs risk analysis to determine whether the incident poses risks to individuals, such as identity theft.

The Corporation then tailors its response to the nature and scope of the risk presented. If the incident results in a risk of identity theft to the person(s) whose data has been breached, the Corporation will provide credit monitoring advice to the person(s) and may offer additional services to resolve the situation if warranted.

The Corporation will provide timely notification to anyone whose personal information has been breached while under the care of the Corporation or its contractors on behalf of the Corporation. The manner of notification is customized to the particular situation of the incident. A point of contact will be designated and provided as part of the notification. The notification must be made in such a way as to not further violate the privacy of the person(s) affected.

If at any time it appears that the loss of data was intentional or that data was the target of the incident, the Office of the Inspector General is notified.





6. COLLECTING PRIVACY DATA

"There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge and consent of the data subject"⁷

6.1
What are the requirements for collecting information covered by the Privacy Act?

The Corporation must evaluate proposals involving collection, use and disclosure of personal information for consistency with the Privacy Act of 1974. System Owners must identify Systems of Records and develop and publish notices as required by the Privacy Act and OMB's implementing policies. See Section 9.

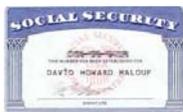
6.2
What is the policy for collecting data via the web?

See section 12 of this Handbook for requirements when collecting information via the web.

6.3
Minimizing the collection of privacy information

You are to collect only the minimum privacy information necessary, and manage it properly to reduce risk to the information and the burden of safeguarding it.

6.4
Social Security Numbers



CNCS is required to minimize the use of social security numbers in Corporation systems and programs. Social security numbers must be eliminated as record identifiers, but should also be eliminated wherever they are not absolutely necessary.

CNCS may not require individuals to disclose their Social Security Number (SSN) unless disclosure would be required under a Federal statute; or any statute, Executive order, or regulation that authorizes any Federal, State, or local agency maintaining a system of records that was in existence and operating prior to January 1, 1975, to request the SSN as a necessary means of verifying the identity of an individual. Individuals asked to voluntarily provide their SSN shall suffer no penalty or denial of benefits for refusing to provide it.

⁷ Peter Swire and Sol Bermann, Information Privacy, 2007

7. PROTECTING PRIVACY DATA



The loss of Personally Identifiable Information (PII) can result in substantial harm, embarrassment, and inconvenience to individuals and may lead to identity theft or other fraudulent use of the information. Because Federal agencies maintain significant amounts of information concerning individuals, we have a special duty to protect that information from loss and misuse. The Corporation has many responsibilities under law to appropriately safeguard PII. Everyone at the Corporation has a role in ensuring those responsibilities are met.

Protection of privacy information relates to protecting PII records, regardless of the media on which that information is stored. Thus, in order to assure the integrity of records, we must consider the handling, storage, and disposition of both physical media (including paper records) and electronic media. Privacy must address all aspects related to assuring the confidentiality and integrity of privacy information.

For the most part, protection of PII is covered under existing information security policies and controls that ensure the confidentiality, integrity, and availability of all “sensitive information”. For example, the OMB requirement to encrypt PII on mobile devices is covered under the ISP Mobile Device Security policy which requires encryption of all sensitive data on mobile devices.

7.1 What are the security requirements for Privacy Information?

There are common and essential requirements across the Corporation for safeguarding all PII in digital form. All PII must be handled and protected as Sensitive information under CNCS' Information Security policies.

The following sections describe some of the key requirements from the security policies that must be applied to privacy data. However, you should read and ensure that you fully understand all of the CNCS information security policies.

7.1.1 Data Transport

Privacy data may only be transported from CNCS premises with written authorization of the information owner. This includes transporting it on a laptop, PDA, flash drive, CD, or other storage device.

7.1.2 Mobile Devices

Any PII on mobile computers (such as laptops) or devices (such as flash drives, PDAs, etc) must be encrypted with an approved encryption solution. OIT is rolling out PointSec to all Corporation-managed PCs and laptops and also configures the encryption for Corporation Blackberries. However, you are responsible for encrypting any other mobile devices that you have. Please contact the OIT Help Desk for assistance with this.

7.1.3 Remote Access

Any system containing PII which provides remote access capabilities must meet the following requirements:

- A "time-out" function requiring user re-authentication after a maximum of 30 minutes of inactivity shall be employed.
- The system must display a warning banner which identifies that the system contains sensitive data and must be protected in accordance with CNCS privacy policies.

**7.1.4
Transmitting or
Transferring Data**

PII data must be protected during transmission. You are required to encrypt all privacy data while it is being transferred. PII, and links to PII, cannot be sent via email unless it is encrypted. The encryption product used must comply with federal requirements, including FIPS 140-2. Please contact the OIT Help Desk for assistance with this.

**7.1.5
Data/System
Access**

System/information owners are responsible for ensuring that access to PII on their systems is only granted to users who require the access for their duties, and that this access is minimized to what is truly necessary.

Access to Corporation-owned PII is only to be granted to personnel who have satisfactorily completed a federal background investigation.

**7.1.6
Paper Records**

Paper-based records containing privacy information must be secured in locked containers or cabinets when not in immediate use. Any portable containers used to transport privacy information should be identifiable by tag, label, or decal with contact.

When no longer needed, any paper containing privacy information must be shredded or placed in the locked shredding bins in the copy rooms.

**7.2
What are the
requirements for
protecting personnel
files**

Managers of automated personnel records shall establish safeguards for data about individuals in those records, including input and output documents, reports, portable media, and online computer systems.

When collecting and handling employee Social Security Numbers:

If Social Security Numbers are collected, they should be collected at the time of an employee's appointment and entered into the human resources and payroll systems.

Required access to Social Security Numbers, including data entry, printing, and screen displays must be conducted in a secure location to protect against unauthorized exposures.

When the Social Security Number is required as a data entry parameter, it must not be displayed on the input screen except when establishing the initial human resources or payroll record. In all other record retrieval and access authorization processes, the Social Security Number must be masked with asterisks or other special characters, similar to the technique used when handling passwords and PINs.



**7.3
What are the
requirements for
using or disclosing
privacy information?**

You must adhere to the following requirements when using or disclosing any privacy data:

- You can only use and disclose privacy information in accordance with the routine uses published in the System of Records Notice for the system or as directed by law, except pursuant to a written request by, or with the prior written consent of, the individual / organization to whom the record

See IPP-07 Systems of Record for more information



pertains. This includes disclosure to contractors, government agencies, other organizations, and individuals.

- You must avoid any unnecessary printing and displaying of SSNs on forms, reports, and computer display screens.
- All disclosures of information containing Social Security Numbers and other personally identifiable data must be made in accordance with established regulations and procedures.
- CNCS will not rent or sell information about individuals.
- All extracts of personal information from Corporation systems must be logged and verified in accordance with IPP-10 Data Extracts (see section 11).
- Those individuals who are authorized to access privacy data must understand their responsibility to protect personal information. This includes securing this information when working from home or another remote location.
- Records shall be maintained that document the disclosure of PII for other than routine use. These records shall include: (A) the date, nature, and purpose of each disclosure of a record or extract to any person or to another agency; and (B) the name and address of the person or agency to whom the disclosure was made. The records of accounting of disclosures shall be retained for five (5) years or the life of the record, whichever is longer, and shall be made available to the individual/company named at their request. The capability shall be provided to inform any person or other agency about any correction or notation of dispute made by the agency of any record that has been disclosed to the person or agency if an accounting of the disclosure was made.

8. TRACKING PRIVACY DATA



In order to protect privacy data, it is crucial to have a complete and accurate inventory of what PII the Corporation collects, stores, and processes; and where this data resides. This section describes the activities that CNCS personnel must perform to maintain an accurate accounting of the PII data that the Corporation possesses.

8.1 Identifying Personally Identifiable Information (PII)

CNCS staff will be asked to assist the Privacy Officer with identifying the PII that is collected, stored, or used by their departments, what the data is used for, and where it is stored. This includes PII in the possession of contractors on behalf of the department. This information will be used to develop an accurate CNCS PII inventory that will provide the basis for many of the components of the CNCS Privacy Program. Staff will also be asked to assist in keeping this inventory up to date by periodically reviewing and updating this information. You are responsible for assisting with these activities as requested and for providing updates to the inventory as you become aware of them.

8.2 Evaluating PII sensitivity

All PII is not equal. Some data elements can have a much more severe adverse impact than others if compromised. For example, compromise of an SSN can be catastrophic because it is used as a primary identifier in so many systems that it is essentially a universal identifier. Release of a person's office telephone number or name would generally have little impact because such data elements are publicly available.

When evaluating PII, the potential impact from unauthorized release or compromise should be assessed. A three-level rating scale (High, Medium, Low) will be used for this rating:

- A High impact element would potentially have a severe impact, affecting an individual directly and/or in multiple systems both within and outside CNCS. The SSN and data concerning an employee's health are examples of High privacy impact data elements.
- A Medium impact data element could have a severe impact on the employee, but its impact on allowing consolidation of data from non-CNCS sources is limited. Examples of Medium impact data elements are encrypted SSNs (because it can not be used to link to other systems) and home telephone numbers.
- Low impact data elements, while meeting the PII definition, are frequently publicly available. Examples of Low impact data elements are an employee's telephone number and work e-mail address.



The items in the PII inventory described in the previous section will be evaluated to determine their sensitivity level. This information will be recorded in the inventory and will be used in determining the handling and security requirements for those data elements.

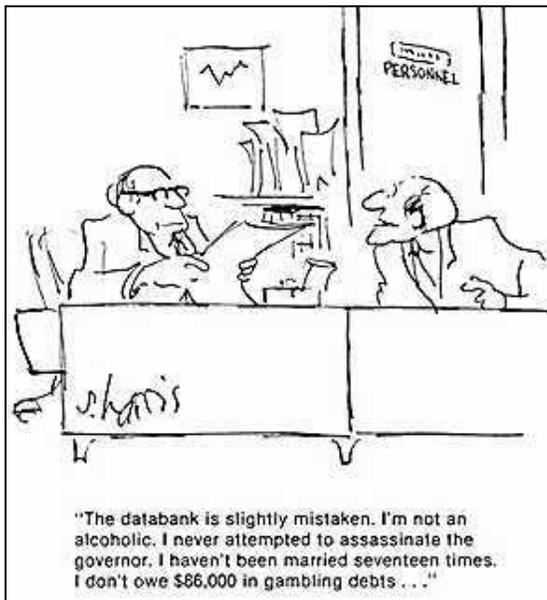
8.3 Minimizing the use of PII



One of the most effective ways to minimize the risks to PII within the Corporation is to minimize the amount of PII collected and the ways it is used. CNCS will conduct periodic reviews of all of the PII and extracts identified in the inventory to determine whether it is really needed. The Corporation will reduce the collection and use of PII to the minimum necessary to perform its functions. Additionally, the printing and displaying of social security numbers and other PII on forms, reports, and computer screens will be minimized to what is absolutely necessary..

The Privacy Officer will issue guidance to help business units with minimizing their use of PII and determining less sensitive alternatives to meet their business requirements. CNCS departments will then be asked to analyze their collection and use of PII and determine any areas where that use can be reduced, eliminated, or replaced with less sensitive information.

Any PII that is no longer needed must be securely disposed of, and the PII inventory updated accordingly. The PII minimization guidance will also assist staff with making future decisions regarding the collection of additional PII or new uses of current PII.





9. SYSTEM OF RECORDS (SOR)

The Privacy Act of 1974 (5 U.S.C. § 552a, the Act) requires agencies to inform the public of the existence of Systems of Records containing personal information, to give individuals access to records about themselves in a system of records, and to manage those records in a way to ensure fairness to individuals in agency programs.

CNCS must ensure that the public is adequately informed about the systems of records the Corporation maintains and the uses that are being made of the records in those systems. The Corporation must periodically review its systems of records and the published notices that describe them to ensure that they are accurate and complete.

9.1 What is a "System of Records"?

A "System of Records" is a collection, or grouping of information, whether paper or electronic, from which personal information about an individual is retrieved by the name of the individual, or by some other identifying number or symbol that is unique to that individual.

9.2 When is a new System Of Records (SOR) created?

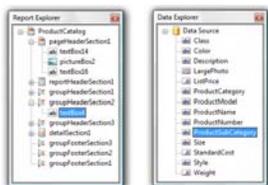
A new System of Records (SOR) is created when any one of the following criteria is met:

- A program, authorized by either a new or an existing statute or Executive Order (EO), requires, for its successful accomplishment, the creation and retrieval of individually identifiable records.
- There is a proposed new use for existing records that is incompatible with the purpose for which the records were originally collected. In this case, all individuals covered by the existing system of records must be notified of the new purpose and routine uses for the records in the SOR and must be provided with a new Privacy Act statement.
- There is a new organization of records, resulting in the consolidation of two or more existing systems into one new ("umbrella") system, whenever the consolidation cannot be classified under a current SOR notice.
- It is discovered that records about individuals are being created and used, and that this activity is not covered by a current, published SOR notice. (This is a "found SOR"). The Office of Management and Budget (OMB) requires the temporary suspension of data collection and disclosure in this case.

9.3 Are there restrictions on what information can be included in a System Of Records?

The following requirements apply to inclusion of information in a system of records:

- Only necessary information relevant to the Corporation's mission may be included.
- The collection of social security numbers (SSNs) should be avoided unless required by statute or some other requirement mandating the use of SSNs.



9.4
What must be done when establishing a new System of Records?

9.5
What must be included in a System of Records Notice (SORN)?



For more information, see IPP-07, System of Records

- Information about political or religious beliefs and activities of individuals will not be maintained.
- Systems of records must not inappropriately combine groups of records which should be segregated. "Groups of records which have different purposes, routine uses, or security requirements, or which are regularly accessed by different members of the agency staff, should be maintained and managed as separate systems of records to avoid lapses in security."
- Corporation systems of records should not duplicate or be combined with those systems which have been designated as "government wide systems of records." A government wide system of records is one for which one agency has regulatory authority over records in the custody of many different agencies. Usually these are federal personnel or administrative records. Such government-wide systems ensure that privacy practices with respect to those records are carried out in accordance with the responsible agency's regulations uniformly across the federal government."

A "System of Record Notice" (SORN) must be issued before CNCS begins to collect personal information for a new system of records. This notice must be published in the Federal Register. The primary purpose of a SORN is to inform the public regarding what types of records the agency maintains, who the records are about, and what uses are made of them.

System Owners must provide detailed information about their System Of Records when drafting a SORN for publication. A SORN template is available from the Privacy Officer.

Each SORN must include:

- Name and location of the system.
- Categories of individuals on whom records are maintained in the system.
- A statement of what types of information are maintained and what the sources of the information are.
- Each routine use of records contained in the system, including the categories of users and the purpose of such use.
- Policies and practices of the agency regarding storage, retrievability, access controls, retention, and disposal of the records.
- Title, name, and business address of the agency official who is responsible for the System Of Records.
- Agency procedures to notify an individual, at his request, how he can gain access to any record pertaining to him contained in the System Of Records, and how (s)he can contest its content.

9.6

What is a "Routine Use"?

A routine use is "the use of such record for a purpose which is compatible with the purpose for which it was collected."⁸ Essentially, when you publish a SORN, you specify the uses that the Corporation can make of the data being collected under that notice. Any use that is not consistent with these published uses is a violation of the Privacy Act.

9.6.1

What are the requirements for reviewing routine uses?

System Owners must review the "routine uses" specified in the SORN for their system to identify any routine uses that are no longer justified, or which are no longer compatible with the purpose for which the information was collected. If a routine use is no longer appropriate, the Corporation should discontinue the use and delete the routine use from the System Of Records notice. If the SORN does not accurately and completely describe the routine uses, the notice must be updated accordingly.

9.6.2

What are some routine uses that should be included in SORNs?

See IPP-07, System of Records, for a list of some general routine uses you may want to consider including in SORNs.

9.7

What is the process for creating and publishing a SORN?

The general process for creating and publishing a System of Records Notice is as follows:

1. The System Owner is responsible for developing a SORN using the CNCS template.
2. The System Owner submits the draft SORN to the Privacy Officer.
3. The Privacy Officer reviews the SORN to verify that it complies with CNCS policies.
4. The System Owner makes any necessary modifications and obtains approval of the Privacy Officer.
5. The System Owner submits the SORN to the Privacy Act Officer for legal review.
6. The System Owner makes any necessary modifications and obtains approval of the Privacy Act Officer.
7. The draft SORN is published in the Federal Register by the Office of General Counsel.
8. If no substantive comments are received within the public comment period, Public Affairs will publish the final SORN on the CNCS public Web site.

⁸ Privacy Act of 1974

9.8

What are the requirements for reviewing and updating SORNs?

Systems of Records and their corresponding notices must be reviewed and updated periodically. SORN reviews will include:

- Verifying that a SORN exists for each System Of Records.
- Ensuring that each System Of Records contains only that information about individuals that is "relevant and necessary" to accomplish an agency purpose.
- Verifying that the original purpose justifying the information collection is still relevant.
- Ensuring that each SORN accurately and completely describes the routine uses, including the categories of users and the purpose of such use.
- Reviewing each routine use to ensure that it continues to be appropriate.
- Checking if changes in Corporation operations or functions have resulted in increased differences among the records that are contained within a common System Of Records or groups of records that once were appropriately combined into a common system may have become sufficiently different that they should be divided into separate systems.
- If it is determined that the SORN does not accurately and completely describe the System Of Records and its routine uses, the System Owner will revise the notice accordingly.

If any information about individuals in a System Of Records is no longer relevant and necessary, or if the entire System Of Records itself is no longer relevant and necessary, then the Corporation will expunge the records (or System Of Records) in accordance with the procedures outlined in the Privacy Act notice(s) and the prescribed record retention schedule approved by the National Archives and Records Administration. The SORN will be accordingly revised (or rescinded).

9.8.1

When is a SOR considered significantly altered?

A SOR is considered to be significantly altered when any of the following alterations are required:

- Increase or change in the number or type of individuals on whom records are maintained (Changes involving the number, rather than the type, of individuals about whom records are kept only need to be reported when the change alters the character and purpose of the SOR).
- Expansion of the type or categories of information maintained (For example, if an employee file is expanded to include data on education and training, this is considered an expansion of the "types or categories of information" maintained).
- Alteration of the manner in which the records are organized, indexed, or retrieved so as to change the nature or scope of these records; such as splitting an existing SOR into two or more different SORs which may occur in a centralization or a decentralization of organizational responsibilities.
- Modification of the purpose for which information in the SOR is used.
- Changed equipment configuration (that is, hardware or software on which the SOR operates to create the potential for either greater or easier access).

9.9

Collecting data for a Privacy Act SOR

System Owners must ensure that information on individuals that is collected and maintained in a SOR is in compliance with Corporation policies and the Privacy Act.

9.9.1

Is notice required when collecting information?

System Owners must ensure that individuals who are asked to provide information to be maintained in a Privacy Act SOR are first presented with a Privacy Act Statement, either on the information collection sheet or screen or via a separate sheet or screen that the individuals can print and retain. Individuals must be notified of the purposes for which their information is collected, and of their rights and obligations regarding supplying the data.

9.10

Accessing Privacy Act records

Staff will limit disclosure of information concerning individuals from a SOR in accordance with routine uses of the records as published in the SORN. Employees may be subject to criminal penalties for willful and intentional violations of the Privacy Act.

System Owners must ensure that a system notification is provided to anyone entering the System of Records. The notice must explain that records in the system are subject to the Privacy Act and that it is illegal to willfully disclose information to individuals not entitled to it.

9.11

Tracking disclosures

System Owners must "keep an accurate accounting" regarding "each disclosure of a record to any person or to another agency," and retain the accounting for at least five years or the life of the record, whichever is longer."⁹ This includes those made under routine uses, and those made pursuant to requests from law enforcement agencies (even though the latter may be exempt from disclosures to the subject individual). Exceptions are made for disclosures made within the agency on a need-to-know basis or disclosure required by the Freedom of Information Act.

The accounting process must be periodically reviewed and updated to ensure effectiveness. This includes reviewing "changes in technology, function, and organization" that may result in accounting procedures becoming outdated or inadequate. The account must be made even if it is at the request or authorization of the individual. The accounting will include at least the following:

- Date of disclosure
- Nature, and purpose of each disclosure
- Name and address of person to whom the data was disclosed

When using or disclosing a record, CNCS must ensure that it is as accurate, relevant, timely, and complete as is reasonably necessary to ensure fairness to the individual.

⁹ 5 U.S.C. § 552a(c)

9.12 Allowing individuals to access and update their information



CNCS must permit individuals access to records pertaining to themselves and to request amendments to those records. Upon request from an individual, CNCS will:

- Inform the individual whether a System Of Records contains records pertaining to them.
- Permit the individual to review any records retrieved by reference to themselves contained in a System Of Records. (This does not pertain to records referenced under someone else's name which include mention of the individual).
- Permit the individual to obtain a copy of any such record at reasonable cost.

Upon receipt of a request from an individual to amend their record, CNCS must:

- Acknowledge receipt of the request in writing within 10 working days and advise the individual of when action will be taken on the request.
- Make corrections to any portion of the information that the individual believes is inaccurate or inform the individual of its refusal to amend the records and the reason for refusal.

9.13 Securing Privacy Act records

The System Owner must ensure the security and confidentiality of the personal information in the System Of Records. Personal information will be treated as "sensitive information" under the CNCS information security policies. Personal information will be protected in accordance with IPP-05 Collecting and Protecting Personal Information (see section 7).

Safeguards must be reviewed annually to ensure that they are appropriate, and updated if necessary. If changes to the safeguards are made, then the System Owner will publish a SORN that reflects the updated safeguards. The notice should explain how access is limited by describing the types of safeguards in place, such as locks, building access controls, passwords, network authentication, etc.

9.14 Are there contract requirements related to SORs?

CNCS will review all agency contracts which provide for maintenance of a System Of Records on behalf of the Corporation to ensure that Privacy Act requirements are included.

The following language is to be inserted into all such contracts:

“As a federal agency, the Corporation for National and Community Service (CNCS) is subject to and complies with the security requirements of the Federal Information Security and Management Act (FISMA). The Contractor shall ensure that services and products provided under a contract resulting from this solicitation shall comply with the Corporation’s information security program and privacy program policies, and Contractor Security Requirements available at http://www.nationalservice.gov/home/security_and_privacy_policy/index.asp.”

10. PRIVACY IMPACT ASSESSMENTS

CNCS must conduct Privacy Impact Assessments (PIAs) for electronic information systems and collections and make them publicly available.

10.1 What is a Privacy Impact Assessment (PIA)?

Privacy Impact Assessment (PIA) is a process for determining the risks and effects of collecting, maintaining, and disseminating Information in Identifiable Form (IIF) in an electronic information system, and for identifying and evaluating protections and alternative processes to mitigate the impact to privacy of collecting the information.

PIAs are conducted to ensure that there is no collection, storage, access, use, or dissemination of identifiable information from or about members of the general public and businesses that is not needed or authorized, and that identifiable information that is collected is adequately protected. PIAs may address issues relating to the integrity and availability of data handled by a system, to the extent these issues are not already adequately addressed in a System Security Plan prepared in accordance with the CNCS information security policy.

10.2 When is a PIA needed?

The E-Government Act requires that agencies conduct a PIA before (i) developing or procuring information technology that collects, maintains, or disseminates information that is in an identifiable form or (ii) initiating a new electronic collection of information that will be collected from 10 or more persons, other than agencies, instrumentalities, or employees of the Federal Government, and will be maintained, or disseminated in an identifiable form, using information technology.

PIAs must be completed for new systems and proposed information collections that contain PII, including systems under development and systems undergoing major modifications. PIAs will be performed and updated as necessary whenever a system change creates new privacy risks. Specifically, a PIA must be performed when:

- Developing or procuring IT systems or investments that collect, maintain, or disseminate information in identifiable form from or about members of the public.
- Initiating, consistent with the Paperwork Reduction Act, a new or significantly revised electronic collection of information in identifiable form for 10 or more persons (excluding agencies, instrumentalities, or employees of the Federal Government).
- Newly applying user-authenticating technology (e.g., password, digital certificate, biometric) to an electronic information system accessed by members of the public.
- Systematically incorporating into existing information systems any databases of IIF purchased or obtained from commercial or public sources.
- Working together with other agencies on shared functions involving significant new uses or exchanges of IIF, such as the cross-cutting E-Government initiatives.
- Altering a business process, resulting in significant new uses or disclosures

10.3
Who decides if a PIA is necessary?

of information or incorporation into the system of additional items of IIF.

- Altering the character of data - when new IIF added to a collection raises the risks to personal privacy (for example, the addition of health or financial information).
- Developing, or issuing a change to, a System of Records Notice.
- Changes are made to information collection authorities, business processes or other factors affecting the collection and handling of IIF.

The System Owner must determine if a PIA is required for the system for which they are responsible. The System Owner must present this rationale to the Privacy Officer for review and approval. The determination as to whether a PIA is required must be documented in the System Security Plan (SSP).

10.4
What must be included in a PIA?

PIAs will analyze and describe:

- what information is to be collected.
- why the information is being collected.
- intended use of the information (e.g., to verify existing data).
- with whom the information will be shared and why.
- what opportunities individuals have to decline to provide information (when providing information is voluntary) or to consent to particular uses of the information (other than required or authorized uses), and how individuals can grant consent.
- how the information will be secured (e.g., administrative and technological controls).
- whether a System Of Records is being created under the Privacy Act.
- what choices the agency made regarding an IT system or collection of information as a result of performing the PIA.

The depth and content of the PIA should be appropriate for the nature of the information to be collected and the size and complexity of the IT system. PIAs conducted for Major information systems should reflect more extensive analyses of:

- the consequences of collection and flow of information.
- the alternatives to collection and handling as designed.
- the appropriate measures to mitigate risks identified for each alternative.
- the rationale for the final design choice or business process.

The Privacy Officer will provide you with the PIA template upon request.

10.5
Who performs a PIA?

If a PIA is determined to be required, then the System Owner, with the support of the Privacy Officer, will ensure that a PIA is completed. However, to be comprehensive and meaningful, PIAs require collaboration by program experts as well as experts in the areas of information technology, security, records management and privacy.

10.6
**How often must
PIAs be reviewed?**

PIAs should be reviewed at least annually. PIAs should be updated if any of the requirements of section 10.2 are met.

10.7
**What is the
approval process for
a PIA?**

The PIA document must be approved by the CNCS “reviewing official” for PIAs. This is currently Rudy Mazariegos, the CNCS Chief Information Officer. System Owners shall submit the fully completed PIA template to the reviewing official. The official, along with the Privacy Officer, will fully review the PIA and make an approval decision.

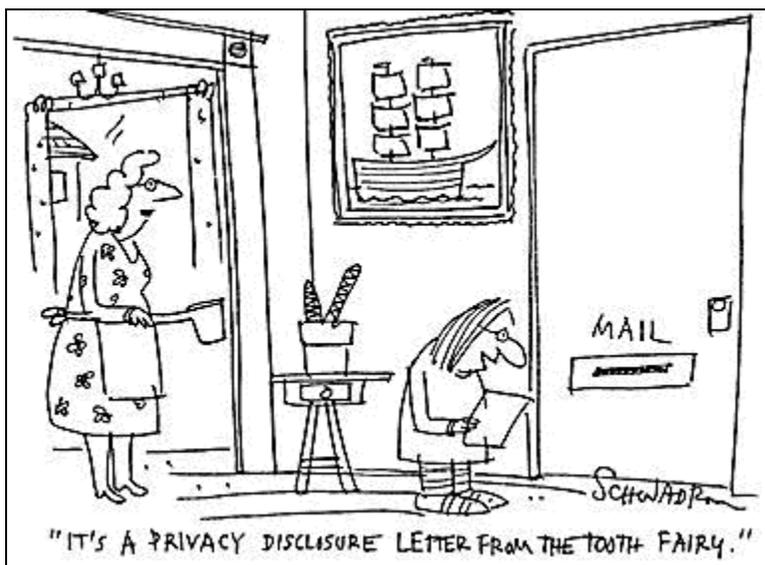
10.8
**Does the PIA need to
be published?**

The E-Government Act and OMB implementing guidance require agencies to make their PIA statements addressing PII available to the public. The PIA statement should not be made publicly available to the extent that the publication would raise security concerns or reveal other sensitive information. A summary of the PIA that omits this sensitive information should be prepared for public availability. Identifiable information should not be included in the PIA statement and cannot be the basis for not making the PIA statement publicly available.

CNCS currently makes its PIAs available through its public web site. Please see http://www.cns.gov/home/security_and_privacy_policy/index.asp for details.

10.9
**Coordinating PIA
completion with
preparing a SORN**

If the information in the system constitutes a Privacy Act SOR for which a new SORN is required, systems owners are encouraged to conduct a PIA concurrently with the SOR Notice required by the Privacy Act, if required, since the PIA and the SOR overlap in content (e.g., the categories of records in the system, the uses of the records, the policies and practices for handling, etc.).





11. DATA EXTRACTS

The Privacy Act establishes a requirement to track extracts of PII. Under the Privacy Act, the rationale for this requirement is to be able to inform extract recipients that the PII provided has changed and to provide the changed data. The Act notes that this is especially important when dealing with PII that might result in an adverse action (e.g., loss of security clearance, poor performance evaluation, and negative hiring decision). The requirement for PII extract tracking was expanded by OMB to ensure that the extracted information is used only for the purpose for which it was provided and is deleted or purged when no longer needed. Additionally, having an accurate accounting of all copies of PII will help to ensure the protection and proper handling of that PII.

11.1 What is a Data Extract?

"Computer readable data extracts" are created when data is retrieved from a database through a query and saved into a separate computer-readable entity such as another database, a spreadsheet, or a text file.¹⁰

While the use of extracts can help productivity, it also exposes the data to numerous risks. Once data has been extracted, it is no longer protected by all of the security measures and procedures that protected it in the original system. Additional measures must be taken to track and protect these extracts and to ensure that they are erased when they are no longer needed. This reduces the likelihood of sensitive information being breached.

11.2 What are the requirements for Data Extracts?

System Owners must ensure that all computer-readable data extracts from databases containing PII are logged and verified, including information on whether the extracted data has been erased within 90 days or that the data's use is still required.

Additionally, extracts should only be created when necessary and authorized. Whenever possible, sensitive information, such as PII, should be scrubbed during extraction.

Sensitive data may not be extracted from a CNCS database via remote access from outside the Corporation's network.

11.2.1 What must be logged?

The logs must include the following:

- date and time of the extract
- name of the system/ database from which the data was extracted
- type of extract
- name of person who performed the extract
- the output of the extract
- whether the extra contains sensitive information

¹⁰ OMB Memorandum M-07-16 Data Extract Frequently Asked Questions (FAQ).

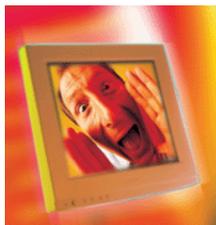
11.2.2 What is verification?

- purpose of the extract
- length of time the extract is needed

Logs should be developed and managed in accordance with NIST Special Publication 800-53 Revision 2, Recommended Security Controls for Federal Information Systems.

At 90 days after creation of the extract, the creator must either attest that the extract has been erased or provide a justification of why the extract is still needed.

- The erasure of extracts containing sensitive information must include sanitization in accordance with CNCS media management policies.
- The Corporation will implement procedures to validate the removal of extracts.
- Extract logs will be updated to include the extract erasure date.



12. WEB SITE PRIVACY

"Web sites are a powerful tool for conveying information on topics relating to activities, objectives, policies and programs of the Federal Government. Web pages provide a simple and speedy means of gaining access to information about the Government, thereby increasing knowledge and understanding of what Government is doing on the people's behalf. Looking ahead, as contemplated for instance by the Government Paperwork Elimination Act, people will conduct more and more business and other activities with the Government electronically. We cannot realize the full potential of the web until people are confident we protect their privacy when they visit our sites... "¹¹ CNCS must protect an individual's right to privacy when personal information is collected on Corporation web sites.

12.1 Can we collect privacy information over the web?

Yes, so long as you comply with CNCS privacy and security policies and all applicable laws. This section summarizes key web privacy policies.

12.1.1 What are the requirements if privacy data is collected?

If Web sites collect PII, Web site owners must ensure that their privacy notices clearly and concisely inform visitors to the site about the data they collect and how that data will be handled.

System Owners must also ensure the security of any PII their Web sites collect.

12.1.2 What is a privacy notice?

A privacy notice is a declaration regarding the Corporation's use of the personal information that it collects from individuals. Such notices state whether third parties may have access to your data and how that data will be used. They also notify web site visitors of their rights under the Privacy Act, where appropriate.

12.1.3 Where must notices be posted?

CNCS will post privacy policies on any agency websites used by the public. Specifically, CNCS will post (or link to) privacy policies at:

- Its principal web site.
- Any known, major entry points to its sites.
- Any web page that collects substantial information in identifiable form.

¹¹ OMB Memorandum M-99-18, Privacy Policies on Federal Web Sites, June 2, 1999.

12.1.4

What needs to be included in notices?

Privacy notices must include:

- Consent to collection and sharing. CNCS will clearly explain where the user may consent to the collection or sharing of information and must notify users of any available mechanism to grant consent.
 - Inform visitors whenever providing requested information is voluntary.
 - Inform visitors how to grant consent for use of voluntarily-provided information.
 - Inform visitors how to grant consent to use mandatorily-provided information for other than statutorily-mandated uses or authorized routine uses under the Privacy Act.
- CNCS will clearly explain an individual's rights under the Privacy Act if solicited information is to be maintained in a Privacy Act System Of Records.
 - Information may be provided in the body of the web privacy policy; via a link to the applicable agency regulation (e.g., Privacy Act regulation and pertinent system notice); or via a link to other official summary of statutory rights (such as the summary of Privacy Act rights in the FOIA/Privacy Act Reference Materials posted by the Federal Consumer Information Center at www.Firstgov.gov).
- Nature, purpose, use, and sharing of information collected.
 - When CNCS collects information subject to the Privacy Act, CNCS will explain what portion of the information is maintained and retrieved by name or personal identifier in a Privacy Act System Of Records and provide a Privacy Act Statement either at the point of collection, or via a link to the agency's general Privacy Policy.
 - Privacy Act Statements must notify users of the authority for, and purpose and use of, the collection of information subject to the Privacy Act; whether providing the information is mandatory or voluntary; and the effects of not providing all or any part of the requested information.
- What information CNCS collects automatically (e.g., user's IP address, location, and time of visit) and identify the use for which it is collected (e.g., site management or security purposes).
- Notice that collected information may be shared and protected as necessary for authorized law enforcement activities.
- With whom, other than law enforcement (as stated above) the information will be shared.
- Information about management, operational and technical controls ensuring the security and confidentiality of personally identifiable records (e.g., access controls, data storage procedures, periodic testing of safeguards, etc.), and in general terms, information about any additional safeguards used to identify and prevent unauthorized attempts to access or cause harm to information and systems. (The statement should be at a

12.1.5 Reviewing and complying with notices

level to inform the public that their information is being protected while not compromising security.)

Privacy policies must be:

- Clearly labeled and easily accessed.
- Written in plain language and made clear and easy to understand.
- Easily accessible by all visitors to a Web site.

You must take care to ensure full adherence with stated privacy notices. For example, if a Corporation web site states that the information provided will not be available to any other entities, you must ensure that no such sharing takes place.

System Owners of web sites must periodically review their web site privacy notices and practices to ensure compliance and accuracy.

12.2 Posting machine readable policies

In accordance with the E-Government Act, CNCS Web-based systems available to the public must incorporate a machine readable privacy statement that alerts users automatically about whether the site privacy practices match their personal privacy preferences so they can make an informed choice about whether to conduct business with CNCS.

12.2.1 What is a "machine readable privacy policy"?

Privacy policy in standardized machine-readable format (also known as "P3P") means a statement about site privacy practices written in a standard computer language (not English text) that can be read automatically by a Web browser.

This allows your browser to check the site's privacy settings against those you have configured in your browser and make a decision about whether the site meets your privacy requirements.

12.2.2 How do I create one?

CNCS has P3P software that is used to create the standard machine readable policies. Please contact the OIT Help Desk for assistance if you need to generate one.

12.3 Collecting information from children

CNCS must adhere to the regulatory requirements of the Children's Online Privacy Protection Act (COPPA) when collecting information electronically from children under age 13.

If any web site is intended for use by children and collects PII from children who are under the age of 13, it must:

- Eliminate the collection of information if the information is not essential to a CNCS program.
- Make reasonable efforts to ensure that parents or legal guardians of children receive notice of the site's information collection practices and obtain verifiable parental consent to those practices before PII is collected from a child.

*For more information on
COPPA, visit
www.coppa.org/coppa.htm*



- Upon request from the parent or legal guardian, the system owner must provide a means that is reasonable under the circumstances for the parent to obtain any personal information collected from that child.
- Ensure that parents are provided with the right to revoke their consent and ask that information about their children be deleted from the site database at any time.
- When a parent revokes consent, the Web site owner must ensure that the collection, use, or disclosure of information from that child is ceased immediately.
- The Web site shall also obtain parental consent when the site:
 - Considers a change to the kinds of information previously collected.
 - Changes how the information is used.
 - Offers the information to new or different third parties.
 - Uses the information in a way that is different than how it was specified when parental consent was originally obtained.
 - Gives a child access to a secondary site that was not originally specified in the Web site notification.
- Ensure that PII is disclosed only to individuals internal to CNCS who have a business requirement for the information or to those individuals external to the Corporation in accordance with "routine uses" published in a Privacy Act SORN.
- Ensure that an exit notice is placed between the COPPA site and any external links stating that CNCS is not responsible for the material found on, or the data collection activities of, the external Web pages. This provides clear notification to both the child and the parent that they are exiting the CNCS domain and that CNCS can no longer guarantee the security of their information.
- Not condition a child's participation in a game, the offering of a prize, or another activity on the child's disclosing of more personal information than is reasonably necessary to participate in such activity.

12.4 Use of cookies and other tracking technology



CNCS will not use persistent cookies or any other means (e.g., web beacons) to track visitors' activity on the Web except for the following exceptions:

- The CNCS CEO may approve the use of persistent tracking technology for a compelling need.
 - When used, CNCS must post clear notice in the web privacy policy of:
 - The nature of the information collected.
 - The purpose and use for the information.
 - Whether and to whom the information will be disclosed.
 - The privacy safeguards applied to the information collected.

- CNCS must report the use of persistent tracking technologies as authorized by the CEO.
- Technology that is used to facilitate a visitor's activity within a single session (e.g., a "session cookie") and does not persist over time is not subject to the prohibition on the use of tracking technology.
- Customization technology (to customize a website at the visitor's request) if approved by the agency head or designee for use (see above) and where the following is posted in the Agency's Privacy Policy:
 - The purpose of the tracking (i.e., customization of the site).
 - That accepting the customizing feature is voluntary.
 - That declining the feature still permits the individual to use the site.
 - The privacy safeguards in place for handling the information collected.

12.4.1

What is a "Cookie"?



A cookie is information created by a Web server and stored on a user's computer. This information lets web sites the user visits keep track of the user's browsing patterns and preferences.

A Persistent Cookie is a cookie that is stored on a user's hard drive until it expires (persistent cookies are set with expiration dates) or until the user deletes the cookie.

A Session Cookie is a temporary cookie that is erased when you close your browser at the end of your surfing session.



13. COMPUTER DATA MATCHING



Inter-agency sharing of information about individuals can be an important tool in improving the efficiency of government programs. By sharing data, agencies can often reduce errors, improve program efficiency, identify and prevent fraud, find intended beneficiaries, evaluate program performance, and reduce information collection burden on the public.

As government increasingly moves to electronic collection and dissemination of data, under the Government Paperwork Elimination Act and other programs, opportunities to share data across agencies will likely increase. With increased focus on data sharing, agencies must pay close attention to handling responsibly their own data and the data they share with or receive from other agencies. When information about individuals is involved, agencies must pay especially close attention to privacy interests and must incorporate measures to safeguard those interests. Prior to any data sharing, agencies must review and meet the Privacy Act requirements for computer matching, including developing a computer matching agreement and publishing notice of the proposed match in the Federal Register. Agencies must also review and meet applicable requirements under other laws, including the Paperwork Reduction Act of 1995. The Computer Matching and Privacy Protection Act (CMPPA), as amended, which amends the Privacy Act, adds certain protections for subjects of Privacy Act records whose records are used in automated matching programs and regulates the conduct of computer matching activities.

13.1 What is "Computer Matching"?

Computer Matching is the electronic comparison of records from two or more automated systems of records maintained by CNCS, other Federal agencies, or a contractor on the Corporation's behalf.

Computer Matching policies apply if the records pertain to applicants, program beneficiaries, or providers of services to programs; and the purpose of the matching is to establish or verify initial or continuing eligibility for Federal benefit programs, verify compliance with the statutory or regulatory requirements of such programs, or recoup payments or delinquent debts under such Federal benefit programs. Computer Matching policies also apply to matches comparing records from automated Federal personnel or payroll systems of records, or such records with automated records of State and local governments.

The following situations are excluded from computer matching policies:

- Statistical matches with the sole purpose of aggregating data stripped of personal identifiers.
- Routine administrative matches using predominantly federal personnel records provided the purpose is not to take adverse action against personnel.
- Law enforcement investigative matches by agencies whose principal function involves enforcement of law.
- Internal matches using only CNCS' own records if the purpose is not to take adverse action against personnel.

13.2
What must be done
before performing data
matching?

- Background investigations.

Information Owners must analyze what data is needed for program purposes and make every effort to ensure that CNCS transfers only the required information.

A Matching Agreement or MOU must be negotiated between the two organizations providing data.

If computer matching will be used to verify program eligibility or to recover delinquent debt, CNCS will:

- Develop procedures for providing notice to the individual at the time of application, and periodically thereafter, that the information they provide may be subject to verification through matching programs, as required by the Matching Act.
- Publish a notice in the Federal Register at least 30 days before conducting the data match, describing the purpose of the match, the records and individuals covered, and other relevant information.

13.2.1
What must be
included in the
MOU?

A Memorandum of Understanding (MOU) or Matching Agreement required for a computer matching program must contain the following:

- Purpose and legal authority.
- Justification and expected results.
- Description of records to be used in the match.
- Procedures for notifying individuals whose records are to be matched.
- Verification methods to be used to independently verify the information obtained through the matching program
- Disposal and retention procedures.
- Security Procedures to be used in protecting the information.
- Records Usage, Duplication, and Redisclosure Restrictions.
- Records Accuracy Assessments.
- Assignment of Responsibilities for posting notices.

13.2.2
What are the
notification
requirements?

Records subjects are to receive direct, constructive, and periodic notices that their records may be matched. Notice must be published in the *Federal Register* at least 30 days prior to conducting a matching program. The notice will contain the names of participating agencies, the purpose of the match, the authority for conducting the match, categories of records and individuals covered (to include identifying the systems of records from which records will be matched), inclusive dates of the matching program, and the address for receipt of public comments .

13.2.3
Receiving data for
matching

If CNCS receives automated records from Privacy Act systems of records of other Federal agencies or from State and local governments to be used in matching programs, CNCS is assumed to be the beneficiary of a matching program and is therefore responsible for the reporting and publishing requirements of the Act.

13.2.4 Sharing data for matching



13.3 CNCS must ensure accuracy of the matched records

13.3.1 Taking adverse action based on

When CNCS is the recipient agency, the component proposing the match will:

- Negotiate and draft the matching agreement.
- Publish the required notice in the *Federal Register* and report the matching program to OMB and specified Congressional Committees.

When receiving data from another agency under a Data Sharing program, CNCS will not re-disclose the data, except where required by law or where the redisclosure is essential to the conduct of the matching program (as allowed under the Matching Act.)

Prior to the sharing of any data, CNCS will ensure that the recipient organization affords the appropriate equivalent level of security controls as maintained by CNCS. Since data security remains the responsibility of the originating agency, procedures should be agreed to in advance that provide for the monitoring over time of the effectiveness of the security controls of the recipient organization.

CNCS will require that the recipient agency certify on a periodic basis that it has examined practices regarding redisclosure and, if necessary, taken corrective action where improper redisclosures have occurred.

If CNCS discloses automated records from a System Of Records to another Federal agency or to a State or local governmental agency to be used in a matching program, CNCS will perform the following:

- if the Corporation is the beneficiary of the match:
 - Negotiate and draft the matching agreement.
 - Negotiate reimbursement to the recipient agency for the costs incurred in publishing notice of the match in the *Federal Register*.
- if the Corporation is not the beneficiary of the match:
 - Participate in negotiating the matching agreement.
 - Review the recipient agency's benefit/cost analysis and supplement the analysis with VA data, as appropriate.
- if the recipient is not a federal agency:
 - Publish the notice in the *Federal Register* and report the match to OMB and Congress.

Because information shared among agencies may be used to deny, reduce, or otherwise adversely affect benefits to individuals, it is critical that CNCS have reasonable procedures to ensure the accuracy of the data shared. To ensure accuracy, CNCS must adhere to the due process requirements found in the Matching Act. Individuals will have the right to access and to request amendment of their records, as required by the Privacy Act.

Before CNCS takes adverse action against an individual based on the results of data produced by a matching program, it must independently verify the data unless there is a determination by the relevant Data Integrity Board, for a limited class of information, that there is a high degree of confidence that the information is

matched data

13.4

**Data Integrity Board
(DIB)**

*For more information, see
IPP-09, Computer Data
Matching*

accurate. At least 30 days before taking adverse action (unless statute or regulation states otherwise), CNCS must also provide notice to the individual of the agency's findings and provide an opportunity to contest those findings.

CNCS will establish a Data Integrity Board (DIB) to oversee and coordinate the Corporation's computer matching program. The DIB will review and approve ongoing matching programs, proposed matches, exclusions, extensions, and renewals. The DIB will ensure that matching agreements and programs are in conformance with provisions of the Act as well as other relevant statutes, regulations, or guidelines, and will assess the benefits and costs of such programs.

Matching agreements should remain in force only as long as necessary to accomplish the specific purpose of the match.

- Agreements automatically expire after 18 months unless the agreement or the DIB specifies a shorter period or the DIB approves an extension not to exceed one year.
- To obtain an extension, the component participating in the match must provide the DIB with certification from each party to the agreement that the program has been conducted in compliance with the agreement and that it will be conducted without change during the extension. Additional information should include the reasons that the match should be extended, including any updated benefit/cost information. GC concurrence will be obtained. The DIB must make its decision to extend a match within three months prior to the expiration date.
- Renewals are treated as initial agreements and require the same documentation. Each benefit/cost analysis must contain updated information based on the actual experience of the match. All documentation must be submitted to the DIB at least two full months prior to expiration of the match.

All matching programs in which the Corporation has participated as either a source or recipient will be reviewed annually.





14. PROGRAM GOVERNANCE

Information Privacy must be managed and governed to reduce risks to CNCS operations and to individuals' private information. CNCS must manage its Information Privacy Program (IPP) to proactively track and mitigate weaknesses, and report on the status of the program as required by OMB.

As a Federal Corporation, CNCS is required by the Privacy Act and other legislation to implement practices to protect personal information. CNCS must conduct reviews verify compliance with privacy requirements, and promptly identify deficiencies and risks. The Corporation is also obligated to take appropriate steps to remedy any deficiencies found. Agencies are also required to maintain appropriate documentation regarding their compliance with information privacy laws, regulations, and policies.

14.1 How does the Privacy Program relate to the Security Program?

The IPP complements the Information Security Program which provides for protection of all of the Corporation's information. Privacy policies and practices will ensure that information is handled in a manner that maximizes both privacy and security.

14.2 How will the IPP be kept up to date?

The IPP will be continuously assessed and updated to ensure that privacy data is adequately protected, federal requirements are being met, and the program is operating as intended. The Corporation will conduct a periodic review (on at least an annual basis) of its policies and processes, and take corrective action as appropriate to ensure that CNCS has adequate safeguards to prevent the intentional or negligent misuse of, or unauthorized access to, personally identifiable information (PII). This review shall address all administrative, technical, and physical means used by the Corporation to control such information.

On a regular basis, the Privacy Officer will check OMB, NIST, and other sources for any new Privacy-related guidance or requirements. For any new privacy law or OMB/NIST privacy guidance that is issued, CNCS will develop a plan and schedule for ensuring compliance with the new requirement(s).

OIT will also meet regularly with the CNCS Office of the Inspector General (OIG) to ensure that the program satisfies audit requirements.

14.3 How will the Corporation track deficiencies

CNCS will maintain a Plan of Actions & Milestones (POA&M) to track identified privacy program deficiencies and remedial actions planned and implemented for those deficiencies. The Privacy POA&M will be integrated with the Information Security POA&Ms and will address Privacy-specific issues not covered under the ISP and System-level POA&Ms. The Privacy Officer will develop and maintain the Privacy POA&M and provide updates to the CISO on a periodic basis for inclusion in FISMA reporting. Any official reports providing specific information on Privacy weaknesses resulting from Inspector General audits, internal reviews, or privacy incidents will be documented as part of the POA&M. The POA&M will be continuously updated as items are completed and new weaknesses discovered so that it reflects the current state of the Corporation's mitigation status.

14.4 OMB reporting

OMB requires annual reports on the Corporations information privacy status under FISMA and the President's Management Agenda Scorecard. Reports will be completed and submitted in accordance with the latest OMB guidance. Additionally, CNCS will provide other applicable privacy-related reports when requested by OMB.

14.5 Privacy Act reviews

CNCS must conduct Privacy Act mandated reviews and will be prepared to report to the Director of OMB on the results of those reviews.

- Section M Contracts - Review every two years a random sample of Corporation contracts that provide for the maintenance of a System Of Records on behalf of the Corporation to accomplish a Corporation function, in order to ensure that the wording of each contract makes the provisions of the Act binding on the contractor and his or her employees. (See 5 U.S.C. 552a(m)(1))
- Records Practices - Review biennially Corporation recordkeeping and disposal policies and practices in order to assure compliance with the Act, paying particular attention to the maintenance of automated records.
- Routine Uses - Review every four years the routine use disclosures associated with each System Of Records in order to ensure that the recipient's use of such records continues to be compatible with the purpose for which the disclosing Corporation collected the information.
- Exemptions - Review every four years each System Of Records for which the Corporation has promulgated exemption rules pursuant to Section (j) or (k) of the Act in order to determine whether such exemption is still needed.
- Matching Programs – Review annually each ongoing matching program in which the Corporation has participated during the year in order to ensure that the requirements of the Act, the OMB guidance, and any Corporation regulations, operating instructions, or guidelines have been met.
- Training - Review biennially Corporation training practices in order to ensure that all Corporation personnel are familiar with the requirements of the Act, with CNCS' implementing regulation, and with any special requirements of their specific jobs.
- Violations - Review biennially the actions of Corporation personnel that have resulted either in the Corporation being found civilly liable under Section (g) of the Act, or an employee being found criminally liable under the provisions of Section (i) of the Act, in order to determine the extent of the problem, and to find the most effective way to prevent recurrence of the problem.
- Systems of Records - Review biennially each System Of Records notice to ensure that it accurately describes the System Of Records. Where minor changes are needed, e.g., the name of the system manager, ensure that an amended notice is published in the Federal Register. Agencies may choose to make one annual comprehensive publication consolidating such minor changes. This requirement is distinguished from and in addition to the requirement to report to OMB and Congress significant changes to systems of records and to publish those changes in the Federal Register.

APPENDIX A: INFORMATION PRIVACY GLOSSARY

<i>Anonymous record (or transaction)</i>	Record (or transaction) whose data cannot be associated with a particular individual, either from the data itself, or by combining the transaction with other data.
<i>Computer Data Matching</i>	This is the expropriation of data maintained by two or more personal data systems, in order to merge previously separate data about individuals.
<i>Cookie</i>	Information created by a Web server and stored on a user's computer. This information lets Web sites the user visits to keep of a user's browsing patterns and preferences.
<i>Data Extract</i>	Data retrieved from a database through a query and saved into a separate computer-readable entity such as another database, a spreadsheet, or a text file
<i>Data Sharing</i>	data matching activities or programs covered under the Computer Matching and Privacy Protection Act.
<i>Disclosure</i>	Release of information contained in a System Of Records to any person (other than the person to whom the information pertains), including any employee of CNCS, or employees of other Federal agencies.
<i>Federal Benefit Program</i>	Any program funded or administered by the Federal government or by any agent or State on behalf of the Federal government, that provides cash or in-kind assistance in the form of payments, grants, loans, or loan guarantees to U.S. citizens or aliens lawfully admitted for permanent residence.
<i>Information Collection</i>	Information collection can occur in any form or format, including the use of report forms; application forms; schedules; questionnaires; surveys; reporting or recordkeeping requirements; contracts; agreements; policy statements; plans; rules or regulations; planning requirements; circulars; directives; instructions; bulletins; requests for proposals or other procurement requirements; interview guides; oral communications; posting, notification, labeling, or similar disclosure requirements; telegraphic or telephonic requests; automated, electronic, mechanical, or other technological collection techniques; standard questionnaires used to monitor compliance with agency requirements; or any other techniques or technological methods used to monitor compliance with agency requirements.
<i>Information in Identifiable Form (IIF)</i>	Information in an IT system or online collection: (i) that directly identifies an individual (e.g., name, address, social security number or other identifying number or code, telephone number, email address, etc.) or (ii) by which an agency intends to identify specific individuals in conjunction with other data elements, i.e., indirect identification. These data element may include a combination of gender, race, birth date, geographic indicator, and other descriptors.
<i>Information Owner</i>	Official with statutory or operational authority for specified information and responsibility for establishing the controls for its generation, collection, processing, dissemination, and disposal.
<i>Information Privacy</i>	The preserving of an individual's right to significantly control the handling and access of information about themselves.
<i>Machine Readable Privacy Policy</i>	A statement about site privacy practices written in eXtensible Markup Language (XML) that can be read automatically by a Web browser. (also known as "P3P")

<i>Members of the Public</i>	Under the E-Gov Act, members of the public are individuals other than government personnel, government contractors, and government consultants and partners. However, under the PRA, government contractors and government consultants and partners may be considered to be members of the public.
<i>Persistent Cookie</i>	A cookie that is stored on a user’s hard drive until it expires (persistent cookies are set with expiration dates) or until the user deletes the cookie.
<i>Personal Identifier</i>	A name or the identifying number, symbol, or other unique identifier such as the SSN or user ID number assigned to an individual.
<i>Personally Identifiable Information</i>	Information about an individual that identifies, links, relates, or is unique to, or describes him or her, or which can be used to distinguish or trace an individual’s identity alone, or when combined with other personal or identifying information. Examples include social security number; age; corporation assigned case number; email address; home/office phone number; driver’s license ID number; biometric Record; finances; education; criminal history; physical attributes; gender, etc.
<i>Plan of Actions and Milestones (POA&M)</i>	A tool that identifies tasks that need to be accomplished. It details resources, milestones, and scheduled completion dates. The purpose of this POA&M is to assist agencies in identifying, assessing, prioritizing, and monitoring the progress of corrective efforts for security weaknesses found in programs and systems.
<i>Privacy Awareness</i>	A state of focused attention on privacy that allows individuals to recognize information privacy concerns and respond accordingly.
<i>Privacy Impact Assessment (PIA)</i>	An analysis of how information is handled: (i) to ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy, (ii) to determine the risks and effects of collecting, maintaining and disseminating IIF in an electronic information system, and (iii) to examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risk.
<i>Privacy Incident</i>	An occurrence that actually or potentially jeopardizes the confidentiality of privacy information, or violates privacy policies, procedures, or laws.
<i>Record</i>	Any item, collection, or grouping of information about an individual that is maintained by an agency and contains his or her name or another personal identifier. This includes, but is not limited to, his education, financial transactions, medical history, and criminal or employment history and that contains his name, or the identifying number, symbol, or other identifying particular assigned to the individual, such as a finger or voice print or a photograph
<i>Routine Use</i>	The use of a record "for a purpose which is compatible with the purpose for which it was collected."
<i>Session cookie</i>	Temporary cookie that is erased when you close your browser at the end of your surfing session.
<i>System of Records</i>	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 the individual

APPENDIX B: ACRONYMS AND ABBREVIATIONS

<i>BII</i>	Business Identifiable Information	<i>OGC</i>	Office of the General Counsel
<i>CEO</i>	Chief Executive Officer	<i>OIG</i>	Office of the Inspector General
<i>CFR</i>	Code of Federal Regulations	<i>OIT</i>	Office of Information Technology
<i>CHCO</i>	Chief Human Capital Officer	<i>OHC</i>	Office of Human Capital
<i>CIO</i>	Chief Information Officer	<i>OMB</i>	Office of Management and Budget
<i>CISO</i>	Chief Information Security Officer	<i>PAO</i>	Privacy Act Officer
<i>CNCS</i>	Corporation for National & Community Service	<i>PL</i>	Public Law
<i>COTR</i>	Contracting Officer’s Technical Representative	<i>PIA</i>	Privacy Impact Assessment
<i>FISMA</i>	Federal Information Security Management Act	<i>PII</i>	Personally Identifiable Information
<i>FOIA</i>	Freedom of Information Act	<i>PO</i>	Privacy Officer
<i>HIPAA</i>	Health Insurance Portability & Accountability Act	<i>POA&M</i>	Plan of Action and Milestones
<i>IIF</i>	Information in Identifiable Form	<i>ROB</i>	Rules of Behavior
<i>IPP</i>	Information Privacy Program	<i>SAOP</i>	Senior Agency Official for Privacy
<i>ISP</i>	Information Security Program	<i>SETA</i>	Security Education, Training & Awareness
<i>IT</i>	Information Technology	<i>SORN</i>	System of Records Notice
<i>NARA</i>	National Archives and Records Administration	<i>SSN</i>	Social Security Number
<i>NIST</i>	National Institute of Standards & Technology	<i>USC</i>	United States Code