Privacy Impact Assessment
for the
SELECTIVE SERVICE SYSTEM
Registration, Compliance and Verification (RCV) System

August 2017

<u>**Contact Point:**</u>
CIO, Selective Service System

<u>**Reviewing Official**</u>
Scott Jones
CIO/Privacy Officer
Selective Service System
[**sjones@sss.gov**](mailto:sjones@sss.gov)
703-605-4128

Abstract

The Selective Service System requires an annual Privacy Impact Assessment be performed on it systems to include all Agency components. This includes all systems that contain personally identifiable information.

All reviewed systems support the Agency's mission of registering men for selective service; all systems are linked to the Agency main strategic goal of registration and support the mission as outlined in the Military Selective Service Act. The Agency seeks to eliminate all non-essential use of PII when possible. Therefore all remaining PII must be in direct support of the Agency's registration mission.

To ensure appropriate safe handling of PII as well as to conform to Federal regulations requiring annual review of PII policies and procedures, the Selective Service System has an active PII program that periodically inspects the Agency's PII-related systems. This annual assessment verifies PII is handled in accordance with regulations and no non-essential PII is maintained.

Overview

The Agency possessed the following PII systems:

PII Inventory			
System Name	**Location**	**Owner**	**Purpose**
GSS	Arlington, VA	NHQ	Personnel management, General File System
IMIS	Arlington, VA	IT	Peacetime management - RFO and SD.
RCV (Registrant Compliance and Verification)	Great Lakes, IL	DMC - Great Lakes, IL	Registrant management - draft registration
FileNet	Arlington, VA	NHQ	Correspondence management
Canon - Enterprise Printing System	Great Lakes	DMC	Printing - hardcopy
Viking Software System	Great Lakes	DMC	Data entry
IVR System	Great Lakes	DMC	Registration support.

These systems collect PII through various means such as a web interface, custom or commercial-off-the-shelf (COTS) applications, vendor-provided applications, or survey forms. Various government agencies such as the Department of Education and the Social Security Administration also supply PII records to SSS. The Agency typically maintains PII records in a relational database management system, but there are also other systems such as the Agency's FileNet application that tracks official correspondence.

To ensure appropriate handling of PII, the Agency undergoes an annual FISMA audit during which the PII procedures are reviewed to ensure an adequate PII program protects the Agency's sensitive data. An outside, third-party audit team reviews these procedures to ensure the SSS conforms to all Federal regulations governing PII management.

Funding for this audit and program comes from the Agency's IT and SPT budgets, and the funding request is part of the annual FY budget submissions to ensure the Agency reserves the necessary resources needed to support the program.

SSS also exchanges data with the Department of Education, Office of Personnel Management, and various Departments of Motor Vehicles in support of the registration mission and other government programs tied to the SSS registration requirement. These records are usually exchanged electronically.

The Military Selective Service Act requires the Agency to register men for a possible selective service. Therefore, the registration database contains PII data for most American men and resident Aliens born after 1959 who were required to register at age 18. The current registration requirement was reinstated in 1980.

SSS uses a Microsoft-based network consisting of Windows Servers and Microsoft SQL Servers. The RCV system consists of a custom application developed specifically for the Agency; IMIS is also a custom in-house system

Section 1.0 Authorities and Other Requirements

1.1 The Military Selective Service Act (MSSA) provides the authority for the SSS to register men for a possible military draft. The MSSA requires Selective Service to record the full name, date-of-birth, Social Security Number, phone number, and mailing address of each registrant.

1.2 What Privacy Act System of Records Notice(s) (SORN(s)) apply to the information?

The following SORNs cover the Agency's PII systems:

1. NCI 147 81 1 = Images of registration documents created for registrants born after 1959. This SORN covers the DMC' microfiche records.

2. NC 147 76 1 = Registration documents (Registration Cards and Classification Records) for registrants born before 1960. This SORN covers registration records for men who registered prior to President Carter reinstating registration in 1980. These records include Vietnam-era and prior records.

3. 76 FR 58321- Privacy Act of 1974; Publications of Notice of Systems of Records.

4. 77 FR 27263 – Computer Matching Between the Selective Service System and the Department of Education.

5. 77 FR 4002 – Privacy Act of 1974; System of Records.

6. 77 FR 4004 – Privacy Act of 1974; Altered System of Records.

7. 76 FR 58321 – Privacy Act of 1974; Publication of Notice of Systems of Records.

1.3 Has a system security plan been completed for the information system(s) supporting the project?

- Yes – the systems are covered by the IT Security Plan and PII handling documents. The general support network is also covered by a certification and accreditation (C&A) performed two years ago – this plan includes the appropriate security controls as designated by NIST.

1.4 Does a records retention schedule approved by the National Archives and Records Administration (NARA) exist?

- Yes – SSS follows the "General" retention plan from NARA.

Section 2.0 Characterization of the Information

2.1 Identify the information the project collects, uses, disseminates, or maintains.

SSS systems to include the RCV system hosting the Registration database collect:
- Full name
- Date of birth
- Gender
- Address
- Social Security Administration number
- Driver's license number
- Phone number

The Registration database assigns a Selective Service Number to a registered individual that uniquely identifies that individual. This number is supplied to external agencies for the purpose of verify registration compliance as well as identify the individual.

2.2 What are the sources of the information and how is the information collected for the project?

SSS receives PII data from various government agencies to include:

- The Social Security Administration (SSA): this data is compared against SSS records for compliance verification. SSS searches the database for individuals who are not listed in the registration database – if an individual is identified, a registration reminder card is sent to advise the individual he has not registered and is required to do so. The SSA database is also used to verify an individual's identity.
- The Department of Education (DoE): these records are submitted as part of the Federal requirement for men to be registered with SSS to qualify for Federal student financial aid. Men can check a "register me" box on their Federal (Pell) financial aid application. If that box is checked, the DoE forwards the data to SSS.
- Various Departments of Motor Vehicles (DMV): numerous States have passed driver license legislation requiring men to register with SSS to qualify for a driver's license. At the time a young man applies for the license, he can elect to register with SSS - the DMV then forwards the records to SSS so they can be added to the registration database.
- Various Universities: Some universities exchange records directly with SSS for the purpose of registration compliance.

2.3 Does the project use information from commercial sources or publicly available data? If so, explain why and how this information is used.

SSS generally does not use commercial entities for registration compliance; however, SSS contracts with *Experian* for a mailing database used to verify addresses.

2.4 Discuss how accuracy of the data is ensured.

SSS compares records between the SSAN database and the Experian database mentioned above.

2.5 Privacy Impact Analysis: Related to Characterization of the Information

<u>Privacy Risk:</u> disclosure of sensitive PII data, possible identity theft, and compromised data integrity – all of these factors would be impacted should PII data be mishandled.

<u>Mitigation:</u> SSS strives to maintain data integrity by ensuring adequate data security practices are followed. This includes maintaining an Internet firewall and various security appliances to protect the data from an Internet-based attack. Also, proper data handling procedures are followed, and the staff receives annual PII training. The Agency's regulation detail PII procedures and requirements, and the staff is required to sign a PII non-disclosure/handling agreement.

The Agency also appointed a privacy officer responsible for reviewing procedures and for conducting annual PII assessments. Training is provided to the staff regarding proper PII management, and the Agency undergoes an annual FISMA audit during which PII policies and procedures are reviewed.

The Agency also adheres to all OMB and NIST guidance such as SP800-53 and FISMA requirements.

Section 3.0 Uses of the Information

3.1 Describe how and why the project uses the information.

SSS uses this PII data to ensure compliance with the Federal requirement for young men to register for a selective service.

3.2 Does the project use technology to conduct electronic searches, queries, or analyses in an electronic database to discover or locate a predictive pattern or an anomaly? If so, state how SSS plans to use such results.

SSS uses electronic searches of PII data – the registration system is a relational database management system with full search capabilities. Also, record exchanges with other government entities are conducted electronically.

As mentioned above, the Agency conducts record searches to identify individuals who may have failed to comply with the Registration requirement. If such a person is identified, a reminder card is mailed to him – the Agency does maintain records recording the date these cards are sent. Also an individual might contact SSS to resolve registration issues, and a record of this contact will be maintained.

The Agency's goal is to promote compliance with the registration requirement – all efforts are aimed at this objective; the goal is not one of prosecution. However, if a man reaches the age of 26 and has not complied with the registration requirement, SSS will forward his name and address to the Department of Justice.

Section 4.0 Notice

4.1 How does the project provide individuals notice prior to the collection of information? If notice is not provided, explain why not.

SSS has published SORNs in the *Federal Register* – see Section 1.2.

The main website hosting On-Line Registration also lists the Agency's privacy policy: http://www.sss.gov/PRIVACY.HTM.

4.2 What opportunities are available for individuals to consent to uses, decline to provide information, or opt out of the project?

The Department of Education financial aid application has a box a person can check to register with Selective Service. This box must be manually checked to demonstrate a conscience effort to register – registration is not automatic. If a person chooses to opt out of the registration requirement, he can leave the box unchecked.

Driver license registration programs often follow the same premise of manually checking a box to demonstrate consent to register. Leaving the box unchecked opts out of the requirement. Each state and territory has policies for automatic opt in, or opt out registration.

Section 5.0 Data Retention by the project

5.1 Explain how long and for what reason the information is retained.

The SSS registration record is maintained indefinitely due to numerous benefits being tied to the registration requirement. For instance, a man might need to prove he registered with SSS to qualify for a Federal job. Because he might apply for that job at any age, SSS must be able to verify his registration at any time. Therefore, SSS must retain the record indefinitely to maintain this capability, so the record cannot be purged from the registration database.

5.2 Privacy Impact Analysis: Related to Retention

The risk of maintaining this information indefinitely is that over time there is a greater chance the PII data might be compromised. An indefinite retainment period increases exposure because the data cannot be purged from the source. SSS takes its responsibility to protect this data seriously, and makes every effort to ensure data integrity. This includes maintaining adequate security, a PII management program, and annual PII management training. No program is foolproof, but SSS makes every effort to ensure the data it's entrusted with remains secure.

Section 6.0 Information Sharing

6.1 Is information shared outside of SSS as part of the normal agency operations? If so, identify the organization(s) and how the information is accessed and how it is to be used.

SSS shares PII data with the Department of Education, various Departments of Motor Vehicles, the Department of Justice, the Social Security Administration, the Office of Personnel Management, and other entities. For a complete list, see *Appendix A*.

This data is used to verify a man's registration status, to register a man with the Agency, or to determine eligibility for benefits tied to the registration requirement. Normally data exchanges are conducted electronically through file exchanges, on-line searches via the Agency's main website at http://www.sss.gov, or through telephonic systems. SSS processes data and provides results in flat files exchanged with other Agencies. The agency also host's a website capable of secure SSL communication to exchange sensitive data. Files can be deposited on the Agency's secure FTP server, and the Agency also supports live calls to its call center operators. All these methods involve using PII data. Also, SSS would share data with the Department of Defense if conscription was enacted.

6.2 Describe how the external sharing noted in 6.1 is compatible with the SORN noted in 1.2.

All agency external sharing is directly linked to registration, compliance, or verification, or associated DoD accessions, or MOUs in the interagency.

6.3 Does the project place limitations on re-dissemination?

Yes – all government entities are prohibited from sharing SSS data without consent. The Memorandums of Understanding impose this limitation.

6.4 Describe how the project maintains a record of any disclosure outside of the Department.

SSS maintains a tracking log of data exchanged with other entities – this log lists the type of data exchanged, the date of exchange, and how the data was exchanged.

Section 7.0 Redress

7.1 What are the procedures that allow individuals to access their information?

Individuals may access their data via the Agency's website at http://www.sss.gov, or via the Agency's telephonic Interactive Voice Response (IVR) system. The Data Management Center also operates a call center with live operators who can assist with a record search. Individuals may submit a letter asking for their registration data. This might be done under the Freedom of Information Act, or an individual might send a request directly to the Public and Congressional Affairs Office.

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

An individual may contact the Agency via written correspondence or directly via the call center to correct erroneous information. The Agency also has a change-of-address webpage that would record corrected mailing addresses. Also, the Public and Congressional Affairs Office can assist with corrections as well.

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

The Agency's main website has contact information and directions: https://www.sss.gov/CONTACT.HTM.

Section 8.0 Auditing and Accountability

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

- SSS undergoes an annual FISMA audit to review PII handling procedures. All deficiencies are reported in the final report, and SSS develops remediation plans to correct the problems. Deficiencies are also tracked on the POA&M.
- The privacy officer also conducts an annual review of Agency system – this review documents all systems maintaining PII data, and the officer develops a remediation plan to correct any deficiencies.
- All Agency personnel are required to adhere to all PII handling practices as outline in the ITSP.
- Annual PII training is provided to the staff – this training details PII procedures and responsibilities.

8.2 Describe what privacy training is provided to users either generally or specifically relevant to this project.

In general, all Agency personnel undergo annual privacy training as part of their annual security training. This training covers PII procedures and responsibilities and instructs the individual on best practices regarding network and PII security. The staff is also required to sign the Rules-of-Behavior form, which also outlines PII handling procedures.

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

SSS position descriptions detail an employee's duties and provide guidance concerning who has access to a given system and what access privileges that person is granted. The Agency follows the practice of issuing the lowest privileges needed to complete the job. No employee can approve his own access privileges, and access is reviewed annually by supervisors and the CIO.

8.4 How does the project review and approve information sharing agreements, MOU, new uses of the information, new access to the system by organization within SSS and the outside?

- MOUs are reviewed annually as part of the FISMA audit mention above. The IT staff and the DMC review MOUs to ensure accuracy, relevancy, and compliance.
- SSS is also required to sign MOUs with various entities exchanging data with the Agency. These documents are also reviewed annually.
- The Agency maintains a list of Agencies SSS has information sharing agreements with, so related MOU are kept current.

Responsible Officials

Scott Jones
CIO
Selective Service System
Operations Directorate, IT
1515 Wilson Blvd.
Arlington, VA 22209

sjones@sss.gov
703-605-4128

Approval Signature

_____

Scott Jones, CIO

Appendix A
Data Exchange Partners

Purpose	Form	External Contact
Verification, Registration, and Compliance	CSB Form 0083	Dept. Educ.
Verification and Compliance	CSB Form 0100	OPM,OFI
Registration	CSB Form 0002	MEPCOM
Registration and Compliance	CSB Form 0002	Immig. (Registration)
Compliance	CSB Form 0037	Immig. (Compliance)
***Data Request* -Supporting Recruitment**	**CSB Form 0006**	**JAMRS - Joint Military Recruiter**
Zip Code cross reference file	CSB Form 0079	USPS (contains no personal information)
Registration	CSB Form 0002	Job Corps
	CSB Form 0146	
Registration	Weekly DMV files	Arizona
Registration	Weekly DMV files	Hawaii
Registration and Compliance	Weekly DMV files	Kentucky
Registration	Weekly DMV files	Louisiana
Registration	Weekly DMV files	South Dakota
Registration	Weekly DMV files	Tennessee
Registration	Weekly DMV files	Alabama
Registration	Weekly DMV files	Colorado
Registration	Weekly DMV files	Delaware
Registration	Weekly DMV files	District of Columbia
Registration	Weekly DMV files	Georgia
Registration	Weekly DMV files	Illinois

Purpose	Form	External Contact
Registration and Compliance	Weekly DMV files	Iowa
Registration	Weekly DMV files	Kansas
Registration	Weekly DMV files	Minnesota
Registration	Weekly DMV files	New Hampshire
Registration and Compliance	Weekly DMV files	New Mexico
Registration	Weekly DMV files	North Carolina
Registration	Weekly DMV files	Ohio
Registration	Weekly DMV files	Oklahoma
Registration	Weekly DMV files	Rhode Island
Registration	Weekly DMV files	Texas
Registration	Weekly DMV files	Utah
Registration	Weekly DMV files	Washington
	CSB Form 0146	
Registration	Monthly DMV files	Arkansas
Registration	Monthly DMV files	Florida
Registration and Compliance	Monthly DMV files	Guam
Registration and Compliance	Monthly DMV files	Idaho
Registration	Monthly DMV files	Indiana
Registration	Monthly DMV files	Mississippi
Registration	Monthly DMV files	Missouri
Registration	Monthly DMV files	Nevada
Registration	Monthly DMV files	New York

Purpose	Form	External Contact
Registration	Monthly DMV files	South Carolina
Registration	Monthly DMV files	Virgin Islands
Registration	Monthly DMV files	Virginia
Registration	Monthly DMV files	West Virginia
Registration	Monthly DMV files	Wisconsin
Data Request - **Supporting Census**	**CSB Form 0152**	**Dept. Of Census**
Compliance	**CSB Form 0065**	**Dept, Justice Referral**
Social Security number reference file	CSB Form 0118	Social Sec. Proc.
Compliance	Compliance DMV	CT State DMV
Compliance	ad-hoc programs	DC State DMV
Compliance	ad-hoc programs	IL State DMV
Compliance	ad-hoc programs	MA State DMV
Compliance	ad-hoc programs	MD State DMV
Compliance	ad-hoc programs	ME State DMV
Compliance	ad-hoc programs	MI State DMV
Compliance	ad-hoc programs	NH State DMV
Compliance	ad-hoc programs	NJ State DMV
Compliance	ad-hoc programs	NY State DMV
Compliance	ad-hoc programs	OH State DMV
Compliance	ad-hoc programs	PA State DMV
Compliance	ad-hoc programs	VT State DMV
Compliance	ad-hoc programs	KY State DMV
Compliance	ad-hoc programs	NC State DMV

Purpose	Form	External Contact
Compliance	ad-hoc programs	PR State DMV
Compliance	ad-hoc programs	TN State DMV
Compliance	ad-hoc programs	TX State DMV
Compliance	ad-hoc programs	WV State DMV
Compliance	ad-hoc programs	AK State DMV
Compliance	ad-hoc programs	AL State DMV
Compliance	ad-hoc programs	AR State DMV
Compliance	ad-hoc programs	AZ State DMV
Compliance	ad-hoc programs	GA State DMV
Compliance	ad-hoc programs	CA State DMV
Compliance	ad-hoc programs	MN State DMV
Compliance	ad-hoc programs	MO State DMV
Compliance	ad-hoc programs	MT State DMV
Compliance	ad-hoc programs	ND State DMV
Compliance	ad-hoc programs	NE State DMV
Compliance	ad-hoc programs	NV State DMV
Compliance	ad-hoc programs	OR State DMV
Compliance	ad-hoc programs	SD State DMV
Compliance	ad-hoc programs	WA State DMV
Compliance	ad-hoc programs	WY State DMV
Compliance	ad-hoc programs	HI State ID Cards
Compliance	CSB Form 0067	Experian (NCOA Match)
Verification	CSB Form 0132	University of New Orleans
Verification	CSB Form 0133	Louisiana State University
Verification	CSB Form 0134	Univ of Louisiana-Lafayette
Verification	CSB Form 0137	University of Cincinnati

Purpose	Form	External Contact
Verification	CSB Form 0139	Lakeland Community College
Verification	CSB Form 0140	Wright State University
Verification	CSB Form 0142	Sinclair Community College
Verification	CSB Form 0147	Kent State University
Verification	CSB Form 0148	University of Dayton
Verification	CSB Form 0149	Youngstown State University
Verification	CSB Form 0150	Ohio University
Verification	CSB Form 0152	University of Akron
Verification	CSB Form 0154	Hocking Technical College
Verification	CSB Form 0155	Ohio State University
Verification	CSB Form 0157	Muskingum College
Verification	CSB Form 0158	University of Toledo
Verification	CSB Form 0159	Terra Community College
Compliance and Registration	CSB FORM 0053	Quarterly DMDC
Compliance and Registration	CSB FORM 0054	Monthly DMDC
Registration	CSB FORM 0061	Active UIC (no personal information) DMDC
Compliance	CSB FORM 0041	Coast Guard
Compliance, Registration and Maintenance	CSB FORM 0084	VADS
Registration	CSB FORM 0106	Reserve Home Address
Registration and Verification	CSB FORM 0153	Alaska Permanent Fund
Verification		Alaska Commission of Education