Privacy Impact Assessment
for the

SELECTIVE SERVICE SYSTEM

IMIS

August 2017

Contact Point:
CIO, Selective Service System

Reviewing Official
Scott Jones
CIO/Privacy Officer
Selective Service System
sjones@sss.gov
703-605-4128

Abstract (IMIS)

OMB A-130, OMB Memorandums 16-06 and 03-22 require an annual Privacy Impact Assessment be performed on its systems - this includes all systems such as the Information Management Information System (IMIS) that contain personally identifiable information.

The IMIS supports the Agency's mission of registering men for a possible military draft, and it is linked to the Agency's main strategic goal of registration as outlined in the Military Selective Service Act. While IMIS doesn't directly handle registration information, it does manage internal business needs such as financial and travel accounting to ensure Reserve Force Officers and State Directors are paid for the service to the Agency.

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 non-essential PII is eliminated to reduce exposure to potential data breaches.

Overview

IMIS collects PII through a web interface and maintains PII records in a relational database management system. 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 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 budget, and the funding request is part of the annual FY budget submissions to ensure the Agency allocates and appropriates funds to support the program.

This document covers only IMIS – remaining PII systems are covered in their own individual Privacy Impact Assessments that can be obtained by writing to the Privacy Officer at:

Privacy Officer
Selective Service System
National Headquarters
1515 Wilson Blvd.
Arlington, VA 22209

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. In support of the registration requirement and to support management and financial planning, IMIS was designed to meet daily business requirements of the Selective Service System.

These requirements include:

- Management of local, district, and national board members, Reserve Force Officers and State Directors, to include personnel, financial, and work assignment management.
- Financial management relating to travel, temporary additional duty, allowances, drill, and expense reimbursements.
- Reporting of local board status of operations such as board member assignments to fulfill staffing requirements.

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

The following SORNs covers IMIS

1. 76 FR 58321- Privacy Act of 1974; Publications of Notice of Systems of Records.

2. 77 FR 4002 – Privacy Act of 1974; System of Records.

3. 77 FR 4004 – Privacy Act of 1974; Altered System of Records.

4. 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 – IMIS is covered by the IT Security Plan and PII handling documents – these documents pertain to the entire network including IMIS.

1.4 Does a record 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.

IMIS collects the following sensitive PII data:

- Full name
- Date of birth
- Gender
- Address
- Social Security Administration number
- Bank account and routing number
- Phone number

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

IMIS PII data comes from:

- Manual entry of PII data from hardcopy records either from SSS Human Resources official documents or official military records.
- Reserve Force Officers or State Directors who manage civil and military performance appraisals.
- Agency Financial and Military Personnel specialists who key data into the system.

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

No – the system does not use commercially available or publically available data.

2.4 Discuss how accuracy of the data is ensured.

Access to the system is limited to only authorized personnel. All system users are vetted by official access authorization requests that are reviewed by the CISO and CIO. Regional offices and the Data Management Center (DMC) must request network access for an individual employee – access rights are documented and reviewed on an annual basis. Also, a Selective Service System e-mail account is a prerequisite to obtaining an IMIS account – this ensures all individuals are vetted per proper documentation and authentication.

2.5 Privacy Impact Analysis: Related to Characterization of the Information

Privacy Risk: Risks entail disclosure of sensitive PII data, possible identity theft, financial risks, and compromised data integrity – all of these factors would be impactors should PII data be mishandled. Unauthorized disclosure of sensitive data of the Agency's military personnel could result in an adverse affect to Agency operations.

Mitigation: SSS maintains data integrity by following accepted data security practices. This includes maintaining an Internet firewall and other security appliances to protect the data from an Internet-based attack. Also, SSS follows data handling procedures, and the Agency receives annual PII training, which is documented in training records. The Agency's regulations detail PII procedures and requirements, and the staff signs a PII non-disclosure/handling agreement upon accepting employment and on an annual basis during yearly security training.

The Agency also employs 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, FIPS-199 and FISMA requirements.

Section 3.0 Uses of the Information

3.1 Describe how and why the project uses the information.

IMIS manages daily operational business needs for the Agency. Requests for reimbursements, financial records, and personnel data are processed by batch and transaction processing. Reports are generated from the database information, stored procedures, queries, and canned reports.

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.

Yes – IMIS performs database searches. The system does little data mining – the main function is to manage financial and personnel records. Simple reports are generated, and there is no need for complex analysis of the data.

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?

Individuals must sign rules-of-behavior detailing their responsibilities before access to the system is granted. A person could consent or decline to submit the requested information at this time. Declining would effectively opt out of the requirement.

Section 5.0 Data Retention by the project

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

The information is retained for the prescribed period determine by the general record schedule.

5.2 Privacy Impact Analysis: Related to Retention

The risk of maintaining this information 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 its data seriously, and makes every effort to ensure data integrity. This includes maintaining adequate security, a PII management program, and annual PII management training. SSS strives to ensure the data it's entrusted with remains secure. Therefore, SSS will periodically review system records to ensure no PII data is maintained unnecessarily, and it will purge PII data when possible. Doing so requires diligence to conduct the periodic review; purging necessary PII data reduces the impact of a data breach and lessens the negatives affects associated with a breach.

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.

Data is shared with the Department of the Interior. See Appendix A.

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

All exchanges are done in support of required business needs as listed in the SORN. Sharing occurs in orders and TDY requests, and in financial transactions. Exchanges are conducted according to established Federal information processing guidelines, such as FIPS-199.

6.3 Does the project place limitations on re-dissemination?

Yes – all government entities are prohibited from sharing SSS data without consent. The Agency maintains Memorandums of Understanding that 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 can contact the CIO and request their PII. Also, a Freedom of Information Act (FOIA) request can be submitted via the Public and Intergovernmental Affairs Office. Individuals must specify what information they require, and the Agency will provide it if possible within the required FOIA response time.

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

Individuals must submit the correction in writing so it can first be verified before official records are updated. Once verified as accurate, the data will be updated via the system's data entry interfaces, and the correction will be noted in a memorandum for record by the CIO.

If submitted information can be changed via the user interfaces, and if the individual has the necessary permission to edit his data, the individual can make the change on his own without notifying others.

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.
- SSS applies the appropriate security controls to its PII data as required under privacy guidelines.
- The Privacy Officer also conducts an annual review of Agency systems – 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, breach, insider threat, and computer training as part of their annual security training. This training covers PII procedures and responsibilities and instructs the individual on best practices regarding network, insider threats 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.

Also, supervisors must validate their assigned employees' access levels on an annual basis. OP/IT then validates that the system reflects the appropriate access levels as determined by that supervisor.

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 Operations IT staff reviews 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**
Department of the Interior	Local Board Extract File	Department of the Interior Help Desk: 1-888-367-1622

Appendix A Data Exchange Partners **Purpose**	**Form**	**External Contact**