Privacy Impact Assessment (PIA) for the

Selective Service System

Enterprise Content Management (ECM) System

September 2022

Introduction

The Selective Service System (SSS) requires PIAs to be conducted and maintained on all IT systems whether already in existence, in development or undergoing modification in order to adequately evaluate privacy risks, ensure the protection of privacy information, and consider privacy implications throughout the information system development life cycle.

Name of Project: Enterprise Content Management (ECM)
Point of Contact Information:

1. Authorizing Official
   Name: Craig Brown
   Title: Acting Director of Selective Service System
   Address: 1515 Wilson Boulevard Arlington, VA 22209
   Phone: (703) 605-4128
   Email: Craig.Brown@sss.gov

2. **Who is the system owner?**
   Name: Nicole Harris
   Title: DMC Director
   Address: P.O. Box 94638 Palatine, IL 60094-4638
   Phone: (847) 688-7920
   Email: Nicole.Harris@sss.gov

3. **Who is the system manager**?
   Name: Ruben Ramos II
   Title: Chief Information Security Officer
   Address: 1515 Wilson Boulevard Arlington, VA 22209
   Phone: (703)-963-2145
   Email: Ruben.Ramos@sss.gov

4. **Who is the Information Systems Security Manager who reviewed this document?**
   Name: Jonathan Kimball
   Title: Information System Security Manager
   Address: 1515 Wilson Boulevard Arlington, VA 22209
   Phone: (703) 605-4123
   Email: Jonathan.Kimball@sss.gov

5. **Who is the Privacy Act Officer?**
   Name: Daniel Mira
   Title: Senior Agency Official for Privacy
   Address: 1515 Wilson Boulevard Arlington, VA 22209
   Phone: (703) 605-4027
   Email: Daniel.Mira@sss.gov

Section 1. General System Information

A. Is a full PIA required?

☒ Yes, information is collected from or maintained on

- ☒ Members of the general public
- ☒ Federal personnel and/or Federal contractors
- ☐ Volunteers
- ☐ All

☐ No: *Information is NOT collected, maintained, or used that is identifiable to the individual in this system. Only sections 1 and 5 of this form are required to be completed.*

B. What is the purpose of the system?

The SSS Enterprise Content Management system (ECM) platform will manage the document workflow and processing automation of the Data Management Center (DMC). The project will develop a Content Services System (CSS) that will manage the Work Item Processing Automation for the Agency. The focus of the project is to enable document capture, OCR (where applicable), access, visibility and routing for status & completion, document archival and destruction, and retrieval based upon the document type and workflow required. These data services include data file storage and processing as well as input from a variety of electronic and paper sources. The ECM includes hardware, software applications, data, communications, and personnel.

The ECM supports the Agency's mission of registering men for selective service; all systems are linked to the Agency's 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.

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 ECM system consists of a custom application developed specifically for the Agency.

C. What is the legal authority?

The Military Selective Service Act (MSSA), 50 U.S.C. App. 3802 et seq. 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.

D. Why is this PIA being completed or modified?

☒ New Information System
☐ New Electronic Collection
☐ Existing Information System under Periodic Review
☐ Merging of Systems
☐ Significantly Modified Information System
☐ Conversion from Paper to Electronic Records
☐ Retiring or Decommissioning a System
☐ Other: *Describe*

E. Is this information system registered in CSAM?
The completed PIA, associated system of records notice(s) and any other supporting artifacts must be entered into the CSAM system for each registered system or application.

☒ Yes: Enterprise Content Management (ECM) System Security Plan
UII Code: There is no UII code for ECM at this time.

☐ No

F. List all minor applications or subsystems that are hosted on this system and covered under this privacy impact assessment.

Subsystem Name	**Purpose**	**Contains PII** *(Yes/No)*	**Describe** *If Yes, provide a description.*
Web server	A web server stores the so-called Unity Forms that are embedded into the SSS website to collect the public's input	No	Used to transfer the PII to the ECM system; does not store the PII.

G. Does this information system or electronic collection require a published Privacy Act System of Records Notice (SORN)?

☒ Yes: *List Privacy Act SORN Identifier(s)*

- The System of Records Notice (SORN) for Registration, Compliance and Verification (RCV) System is located in the Federal Registry Vol 82. No125, paged 29971-29972

☐ No

Section 2. Summary of System Data

A. What PII will be collected? Indicate all that apply.

Identify all the categories of PII that will be collected, stored, used, maintained or disseminated. Describe any additional categories of PII not already indicated, as well as any new information that is created (for example, an analysis or report), and describe how this is done and the purpose of that information.

☒ Full Name
☒ Gender
☒ Birth Date
☐Driver's License
☐ Race/Ethnicity
☒ Social Security Account Number (SSAN)
☒ Telephone Number
☒ Personal Email Address
☒ Mailing/Home Address
☒ Other: *Specify the PII collected –*
Military Duty Status
Citizenship/Immigration (alien ID) status
Date of Death
Selective Service Number
Compliance Pin

B. What is the source for the PII collected? Indicate all that apply.

☒ Individual
☐ Federal agency
☐ Tribal agency
☐ Local agency
☐ Third-party source
☐ State agency
☐ Other: *Describe*

Currently, there is no direct integration between the ECM system and any external system; all connections are internal. Data is transmitted to and from other state and federal agencies such as educational institutions sending data to the ECM system requesting an individual's registration status.

C. How will the information be collected? Indicate all that apply.

☒ Paper Format
Mailing completed registration or change of address forms
☒ Email
Sending completed registration and change of address forms via email
☐ Face-to-Face Contact
☒ Web site
☐ Fax
☒ Telephone Interview
☐ Information Shared Between Systems. *Describe*
☐ Other: *Describe*

D. What is the intended use of the PII collected?

SSS uses this PII data to ensure compliance with the Federal requirement for young men to register for selective service. PII data is used to perform Selective Service System's (SSS) mission-critical business functions related to ECM. The information is used for conscription during a national emergency authorized by Congress and the U.S. President.

E. With whom will the PII be shared, both within SSS and outside SSS? Indicate all that apply.

☒ Within the Bureau/Office: *Describe the bureau/office and how the data will be used.*
The documents containing PII are indexed with that PII information and are stored in a single searchable repository, so employees with the proper access can search and retrieve the document. The PII data collected on the forms are passed through to the RCV, thus RCV users with the proper read rights can view the data

☐ Other Bureaus/Offices: *Describe the bureau/office and how the data will be used.*

☐ Other Federal Agencies: *Describe the federal agency and how the data will be used.*

☐ Tribal, State or Local Agencies: *Describe the Tribal, state, or local agencies and how the data will be used.*

☐ Contractor: *Describe the contractor and how the data will be used.*

☐ Other Third-Party Sources: *Describe the third-party source and how the data will be used.*

F. Do individuals have the opportunity to decline to provide information or to consent to the specific uses of their PII?

☐ Yes: *Describe the method by which individuals can decline to provide information or how individuals consent to specific uses.*

☒ No: *State the reason why individuals cannot object or why individuals cannot give or withhold their consent.*

Individuals who send us forms are in compliance with the law. There is a Privacy Act Statement on each form to inform the users of the purpose of the data being collected. This is outside of the ECM scope, ECM itself as a system is just a conduit to the RCV for the PII data.

G. What information is provided to an individual when asked to provide PII data? Indicate all that apply.

☒ Privacy Act Statement: *Describe each applicable format.*
Privacy Act Statement is printed on the back of the Compliance letter and Form 1 and Form 2.

☐ Privacy Notice: *Describe each applicable format.*

☐ Other: *Describe each applicable format.*

☐ None

H. How will the data be retrieved? List the identifiers that will be used to retrieve information (e.g., name, case number, etc.).

Data can be retrieved from ECM () using one or more of the following elements:

1. Selective Service Number
2. Social Security Account Number
3. Document Locator Number (internally only)
4. Last Name
5. Given Name
6. Date of Birth
7. Address (internally only)
8. Compliance PIN
9. email address

I. Will reports be produced on individuals?

☒ Yes: *What will be the use of these reports? Who will have access to them?*

The ECM system can be queried using the above-mentioned criteria. The ECM system produces pulls a list of scanned images based on the matching criteria of the search.

The ECM system also produces summary reports on the statistical data such as the number of records by document type per time period, as well as workload-related reports on system users

☐ No

Section 3. Attributes of System Data

A. How will data collected from sources other than SSS records be verified for accuracy?

For paper-based documents, the AnyDoc software will process a scanned image utilizing Optical character recognition (OCR) capability. It will flag an area with possible erroneous data, so the Data Validation Team will make a proper correction. Also, during further processing, the document is going to be reviewed by the Data Validation Team

For data collected by Unity form, certain validations are performed on the form (like date format, zip code), while others are validated by web services interfacing with RCV build-in validation function

B. How will data be checked for completeness?

Data requirements such as whether a data element is required, the type of data, and the length of the data elements are specified for registration, compliance, and verification processes. These data requirements are enforced when data is interfaced with RCV utilizing web services or visually reviewed by document services personnel if character recognition software has a low confidence.

C. What procedures are taken to ensure the data is current? Identify the process or name the document (e.g., data models).

ECM is interfacing with RCV to pull the data from the system of record when necessary for the proper indexing of the document only. For example, when an SSAN is not listed on the document, but the RCV contains that information for that individual, that information can be brought to the document on the RCV by the re-indexing function
Otherwise, the information that is contained on the document under the process in ECM is considered the current data.

D. What are the retention periods for data in the system? Identify the associated records retention schedule for the records in this system.

Currently, no retention policy is created to retain records for a specific period of time, thus all documents are retained indefinitely.
ECM will follow the guidance of the Record Retention Operation Memorandum when it's developed and published

E. What are the procedures for the disposition of the data at the end of the retention period? Where are the procedures documented?

The ECM will implement the automatic deletion process once the Record Retention Operation Memorandum is in place

F. Briefly describe privacy risks and how information handling practices at each stage of the "information lifecycle" (i.e., collection, use, retention, processing, disclosure, and destruction) affect individual privacy.

The Selective Service System documents privacy risks and handling in the organization's Privacy Program Plan.

Section 4. PIA Risk Review

A. Is the use of the data both relevant and necessary to the purpose for which the system is being designed?

☒ Yes: *Explanation*

SSS uses this PII data to ensure compliance with the Federal requirement for young men to register for a selective service. PII data is used to perform Selective Service System's (SSS) mission-critical business functions related to Registration, Compliance, and Verification.

☐ No

B. Does this system or electronic collection derive new data or create previously unavailable data about an individual through data aggregation?

☐ Yes: *Explain what risks are introduced by this data aggregation and how these risks will be mitigated.*

☒ No

C. Will the new data be placed in the individual's record?

☒ Yes: *Explanation*

Yes, the ECM system interfaces with the system of record system (RCV), and utilize web services to either insert a new registration record or update an existing record with the latest information

☐ No

D. Can the system make determinations about individuals that would not be possible without the new data?

☐ Yes: *Explanation*

☒ No

E. How will the new data be verified for relevance and accuracy?

See Section 3. Attributes of System Data, para. A and para. B

F. Are the data or the processes being consolidated?

☐ Yes, data is being consolidated. *Describe the controls that are in place to protect the data from unauthorized access or use.*

☐ Yes, processes are being consolidated. *Describe the controls that are in place to protect the data from unauthorized access or use.*

☒ No, data or processes are not being consolidated.

G. Who will have access to data in the system or electronic collection? Indicate all that apply.

☒ Users
☒ Contractors
☒ Developers
☒ System Administrator
☐ Other: *Describe*

H. How is user access to data determined? Will users have access to all data or will access be restricted?

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 System Owner.

Access to each function that is implemented in the ECM system is secured through user roles and access rights. Each user goes through an enrollment process per Manager's ad-hoc request which ensures that access to a certain function is given only to appropriate staff members.

I. Are contractors involved with the design and/or development of the system, or will they be involved with the maintenance of the system?

☒ Yes. *Were Privacy Act contract clauses included in their contracts and other regulatory measures addressed?*

Contractors are utilized for the design, development, and maintenance of the system. The Privacy Act contract clause is a standard section in all contracts.

☐ No

J. Is the system using technologies in ways that the SSS has not previously employed (e.g., monitoring software, SmartCards or Caller ID)?

☒ Yes. *Explanation*

The ECM is a third-party tool that allows the agency to conduct improved Enterprise-level Electronic Content Management. Some of the new technological functions:

a. Optical character recognition (OCR)/ Intelligent Character Recognition (ICR) capability
b. Cataloging documents with attached searchable metadata

☐ No

K. Will this system provide the capability to identify, locate and monitor individuals?

☐ Yes. *Explanation*

☒ No

L. What kinds of information are collected as a function of the monitoring of individuals?

The ECM system records all end-user actions in an audit log which include: user id/name, type of action, date, and time of action. Using this information, when needed, the following can be determined:

1. Who accessed the system
2. What function of the system was used
3. When the system was used

M. What controls will be used to prevent unauthorized monitoring?

Only users in a certain user group can view the report of employees' level of performance

N. How will the PII be secured?

(1) Physical Controls. Indicate all that apply.

☒ Security Guards
☒ Key Guards
☒ Locked File Cabinets
☒ Secured Facility
☒ Closed Circuit Television
☐ Cipher Locks
☒ Identification Badges
☐ Safes
☐ Combination Locks
☒ Locked Offices/Desk
☐ Other. *Describe*

(2) Technical Controls. Indicate all that apply.

☒ Password
☒ Firewall
☒ Encryption
☒ User Identification
☐ Biometrics
☒ Intrusion Detection System (IDS)
☒ Virtual Private Network (VPN)
☒ Public Key Infrastructure (PKI) Certificates
☒ Personal Identity Verification (PIV) Card
☐ Other. *Describe*

(3) Administrative Controls. Indicate all that apply.

☐ Periodic Security Audits
☒ Backups Secured Off-site
☒ Rules of Behavior
☒ Role-Based Training
☒ Regular Monitoring of Users' Security Practices
☒ Methods to Ensure Only Authorized Personnel Have Access to PII
☒ Encryption of Backups Containing Sensitive Data
☒ Cyber Awareness Challenge
☒ Identifying and Safeguarding PII
☐ Phishing Awareness
☒ Insider Threat Awareness
☒ Privacy Act - PII Rules of Behavior
☒ General Information Technology Security Program Rules of Behavior
☒ ECM System Rules of Behavior
☒ Mandatory Security, Privacy, and Records Management Training
☐ Other. *Describe*

O. Who will be responsible for protecting the privacy rights of the public and employees? This includes officials responsible for addressing Privacy Act complaints and requests for redress or amendment of records.

The ECM Information System Owner is responsible for oversight and management of the ECM security controls and the protection of personal information processed and stored by ECM. The Information System Owner is responsible for ensuring adequate safeguards are implemented to protect individual privacy in compliance with Federal laws and policies for the data managed and stored in ECM. The Information System Owner is responsible for protecting the privacy rights of the public and employees for the information they collect, maintain, and use in the system, and for meeting the requirements of the Privacy Act, including providing adequate notice, making decisions on Privacy Act requests for notification, access, and amendments, as well as processing complaints, in consultation with the SSS Privacy Officer.

P. Who is responsible for assuring proper use of the data and for reporting the loss, compromise, unauthorized disclosure, or unauthorized access of privacy protected information?

The ECM System Owner and Business Owners have the overall responsibility for daily operational oversight and management of the system's security and privacy controls, for ensuring to the greatest possible extent that the data is properly managed and that all access to the data has been granted in a secure and auditable manner. The ECM Information System Owner, the Information System Security Officer, and any authorized users are responsible for ensuring that any loss, compromise, unauthorized access, or disclosure of PII reporting is in accordance with Federal policy and established SSS procedures, and appropriate remedial

activities are taken to mitigate any impact to individuals, in coordination with the SSS Privacy Officer. Whoever has access to the ECM system and agencies participating in the use of the ECM system are responsible for protecting the privacy rights of the public and employees.

Section 5. Review and Approval

PIAs for Bureau or Office level systems must be signed by the designated Information System Owner, Information System Security Officer, and Bureau Privacy Officer, and approved by the Bureau Assistant Director for Information Resources as the Reviewing Official. Department-wide PIAs must be signed by the designated Information System Owner, Information System Security Officer, and Departmental Privacy Officer, and approved by the SSS Chief Information Officer/Senior Agency Official for Privacy as the Reviewing Official.

Chief information officer (CIO):

Scott Jones	SCOTT JONES Digitally signed by SCOTT JONES Date: 2022.10.27 08:43:44 -04'00'	10/27/2022
Scott Jones	Signature	Date

Chief Information Security Officer (CISO):

Ruben Ramos II	Ruben Ramos II Digitally signed by Ruben Ramos II Date: 2022.10.26 12:59:50 -04'00'	10/26/2022
Ruben, Ramos II	Signature	Date

System Owner (SO):

Steve Panich on behalf of Nicole Harris	VYACHESLAV PANICH Digitally signed by VYACHESLAV PANICH Date: 2022.10.19 10:57:59 -05'00'	10/19/2022
Nicole Harris	Signature	Date

Senior Agency Official for Privacy (SAOP):

Daniel Mira	DANIEL MIRA Digitally signed by DANIEL MIRA Date: 2022.10.26 12:36:33 -04'00'	10/26/2022
Daniel Mira	Signature	Date