



**Registration, Compliance and Verification
(RCV) Cloud Modernization**

Privacy Impact Assessment (PIA)

**Selective Service System
National Headquarters
Arlington, VA 22209-2425**

April 14, 2025

System Information

Name of System, Project, or Program: RCV Cloud Modernization (RCV)

OMB Unique Identifier: N/A

Contact Information

1. Authorizing Official

Name: Craig T. Brown

Title: Acting Director of Selective Service System

Address: 1501 Wilson Boulevard Arlington, VA 22209

Phone: (703) 605-4082

Email: craig.brown@sss.gov

2. Who is the system owner?

Name: Harry S. Kantor

Title: System Owner

Address: 1501 Wilson Boulevard

Arlington, VA 22209

Phone: (703) 605-4122

Email: Harry.Kantor@sss.gov

3. Who is the system manager?

Name: Steve Panich

Title: Division Manager

Address: Data Management Center, 2834 Green Bay RD,

Building 3400, Great Lakes, Illinois 60088

Phone: (847) 688-7904

Email: Vyacheslav.Panich@sss.gov

4. Who is the Privacy Act Officer?

Name: Alma Cruz

Title: Senior Agency Official for Privacy

Address: 1501 Wilson Boulevard Arlington, VA 22209

Phone: (703) 605-4036

Email: Alma.Cruz@sss.gov

5. Who is the IT Reviewing Official? (CIO Name, title, organization, phone, email, address).

Name: Jeff Steinlage

Title: Acting Chief Information Officer

Address: 1501 Wilson Boulevard Arlington, VA 22209 Arlington, VA 22209

Phone: 571-867-8044

Email: Jeff.Steinlage@sss.gov

System Application/General Information

1. Does this system contain any information in identifiable form?

Yes. The RCV system contains the following information:

- a) First Name
- b) Last Name
- c) Middle Name
- d) Suffix
- e) Social Security Number
- f) Date of Birth
- g) Street Address
- h) E-mail Address
- i) Selective Service Number
- j) Phone Number

2. What is the purpose of the system/application?

The purpose of the RCV system is to perform Selective Service System's (SSS) mission critical business functions related to Registration, Compliance, and Verification, (RCV). The RCV system is an Intranet application used by only authorized SSS' personnel. It provides a central repository for all data related to active registrants and potential violators. The RCV system also interfaces with the following systems:

- a) SSS' public Web site: to support on-line registration, address update, and verification.
- b) SSS' Interactive Voice Response (IVR) system: to support registration and verification services over the phone.
- c) AAMVA's UNI: to receive data from Department of Motor Vehicles
- d) The Selective Service System's Verification Web Service
- e) The Selective Service System's Enterprise Content Management (ECM) System

3. What legal authority authorizes the purchase or development of this system/application?

The RCV system supports the SSS mission, which is governed by the "Military Selective Service Act".

4. Under which Privacy Act SORN does the system operate? (Provide the system name and unique system identifier.)

The System of Records Notice (SORN) for the RCV system is located in the Federal Registry / Vol 65, No 184, page 57215-57222.

Data in the System

1. What categories of individuals are covered in the system?

The RCV system contains information on the following types of individuals:

- a. Men who are at least 18 years old and registered with SSS.
- b. Men who are at least 18 years old and should have registered with SSS but did not register.

- c. Men who are at least 18 years and exempt from the Military Selective Service Act
- d. Men who are potential violators of the Military Selective Service Act
- e. Men who are younger than 18-year-old in early status until they are within age to be registered

2. What are the sources of information in the system?

- a. Is the source of the information from the individual or is it taken from another source? If not directly from the individual, then what other source?**

Individuals submit information to SSS through the following methods:

- i. Mailing completed registration forms
- ii. Mailing completed change of address forms
- iii. Completing online registration using SSS public Web site
- iv. Updating address information using SSS public Web site
- v. Registering with SSS using the IVR
- vi. Updating registration information via a phone call with a SSS representative and/or through miscellaneous correspondence

Individuals also submit the information indirectly to SSS through the following agencies by providing their consent on various forms:

- i. Department Of Education (historical data only)
- ii. States' Departments of Motor Vehicles
- iii. U.S. Military Entrance Processing Command
- iv. Military Academies (historical data only)
- v. U.S. Citizenship and Immigration Services
- vi. Job Corps of the U.S. Department of Labor
- vii. Alaska Permanent Fund
- viii. Georgia Student Finance Commission (historical data only)
- ix. Defense Manpower Data Center of the Department of Defense

- b. What Federal agencies are providing data for use in the system?**

The RCV system receives data from the following federal agencies to execute registration, compliance, and verification business functions:

- i. Defense Manpower Data Center of the Department of Defense
- ii. Department of Veterans Affairs
- iii. Job Corps of the U.S. Department of Labor
- iv. Social Security Administration
- v. U.S. Citizenship and Immigration Services
- vi. U.S. Military Entrance Processing Command
- vii. U.S Post Office

- c. What State and/or local agencies are providing data for use in the system?**

The RCV system receives data from the following state and/or agencies to execute registration, compliance, and verification business functions:

- i. State Department of Motor Vehicles

- a. Alabama
- b. Arizona
- c. Arkansas
- d. California
- e. Colorado
- f. Connecticut
- g. Delaware
- h. District of Columbia
- i. Florida
- j. Georgia
- k. Guam
- l. Hawaii
- m. Idaho
- n. Illinois
- o. Indiana
- p. Iowa
- q. Kansas
- r. Kentucky
- s. Louisiana
- t. Maine
- u. Maryland
- v. Massachusetts
- w. Michigan
- x. Minnesota
- y. Mississippi
- z. Missouri
- aa. Montana
- bb. Nebraska
- cc. Nevada
- dd. New Hampshire
- ee. New Jersey
- ff. New Mexico
- gg. New York
- hh. North Carolina
- ii. North Dakota
- jj. Ohio
- kk. Oklahoma
- ll. Oregon
- mm. Pennsylvania
- nn. Puerto Rico
- oo. Rhode Island
- pp. South Carolina
- qq. South Dakota
- rr. Tennessee
- ss. Texas
- tt. Utah
- uu. Vermont
- vv. Virgin Islands

- ww. Virginia
- xx. Washington
- yy. West Virginia
- zz. Wisconsin
- aaa. Wyoming
- ii. Alaska Permanent Fund

d. What information will be collected from the employee and the public?

The RCV system does not collect information from employees. The following information is collected from the public when an individual is registered:

- i. Gender
- ii. Name: First Name, Middle Name, Last Name, Suffix
- iii. Address
- iv. Social Security Account Number
- v. Date of Birth
- vi. E-mail Address
- vii. Phone Number

3. Accuracy, Timelines, and Reliability

a. How will data collected from sources other than bureau records be verified for accuracy?

Data received from all sources goes through consistent data validation checks. Entries that fail data validation checks are either flagged for further investigation or flagged not to be used in processing.

b. How will data be checked for completeness?

Data requirements such as whether a data element is required, the type of data, and length of the data elements are specified for registration, compliance, and verification processes. These data requirements are enforced when data is entered, processed, and stored.

c. Is the data current? What steps or procedures are taken to ensure the data is current and not out-of-date? Name the document (e.g., data models.)

The data in the RCV system is kept up to date by various supporting avenues.

- i. Individuals submit changes using standard SSS forms.
- ii. Individuals use the SSS' public website to update addresses.
- iii. Individuals call SSS to update information.
- iv. External sources that are listed above send information periodically.
- v. RCV sends information to Verimove.

d. Are the data elements described in detail and documented? If yes, what is the name of the document?

Data elements are fully specified in the Data Dictionary of the RCV system (RCV-DataDictionary.docx).

Attributes of the Data

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

Yes. The data collected is required to implement the Military Selective Service Act.

2. Will the system derive new data or create previously unavailable data about an individual through aggregation from the information collected, and how will this be maintained and filed?

The RCV system utilizes the individual's year of birth while creating the Selective Service Number. This number is communicated to the individual and is used in subsequent inquiries related to the individual's registration status.

When individuals submit their information on paper forms, corresponding electronic records are created (which will be loaded into the RCV system).

During this process, each record is given a Document Locator Number, which is stored in the RCV system.

When an individual is added to the potential violator list, the RCV system generates a Personal Identification Number (PIN), which is communicated to the individual, allowing the person to register with SSS. The individual will have the option to register using the PIN.

A few external data sources do not provide all components of an individual's name in standard form. For example, instead of providing last-name, first-name, middle-name, suffix in individual data elements, a full-name is provided in a single data element. In such cases, individual components of the name are extracted and stored in individual data elements.

The given-name of an individual is derived by the RCV system by concatenating the first name and the middle-name, separated by a space.

The RCV system receives data related to the individual's military service record, immigration status, and death record. The RCV system updates the individual's record with the new information.

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

Yes.

4. Can the system make determinations about employees/public that would not be possible without the new data?

The Selective Service Number is needed to determine the registration status of an individual. Individual components of the name are also needed to process records of registrants and potential violators of the Military Selective Service Act.

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

The uniqueness of the Selective Service Number is enforced by implementing a unique-index constraint in the database. If any data validation rules fail, the

corresponding records are marked to be resolved by the staff.

6. If the data is being consolidated, what controls are in place to protect the data from unauthorized access or use?

Access to each function that is implemented in the RCV system is secured through user role and access rights. Each user goes through an enrollment process which ensures that access is given only to appropriate staff members. Data in transit and at rest is encrypted.

7. If processes are being consolidated, are the proper controls remaining in place to protect the data and prevent unauthorized access? Explain.

N/A

8. How will the data be retrieved? Does a personal identifier retrieve the data? If yes, explain and list the identifiers that will be used to retrieve information on the individual.

Data is retrieved using one or more of the following elements:

- a. Selective Service Number
- b. Social Security Account Number
- c. Document Locator Number
- d. Last Name
- e. Given Name
- f. Date of Birth
- g. Address
- h. PIN
- i. E-mail address

9. What kinds of reports can be produced on individuals? What will be the use of these reports? Who will have access to them?

The RCV system can be queried using the above-mentioned criteria. The RCV system produces the following types of data extract files:

- a. List of individuals who are eligible for military draft to be used by the Department of Defense for marketing, recruiting, and drafting, when required.
- b. List of individuals who are potential violators of the Military Selective Service Act to be used by the Department of Justice to enforce the law.
- c. A subset of individuals who are potential violators of the Military Service Act and whose addresses need to be verified through the National Change of Address service.

The RCV system also produces summary reports on the number of registrations by region, state, year, source, special projects, etc.

Maintenance and Administrative Controls

1. If the system is operated on more than one site, how will consistent use of the system and data be maintained in all sites?

The RCV system is hosted in an AWS Cloud. All data is stored in Amazon's RDS service, which handles data consistency across availability zones and regions. Data integrity is maintained by enforcing data validation rules; implementing data constraints such as foreign keys and unique indexes; and implementing transaction commit-rollback mechanism.

2. What are the retention periods of data in this system?

Records for the RCV system are retained according to the System of Records Notice (SORN) in the Federal Registry / Vol 65, No 184, page 57215-57222. Currently, no automated archival procedures are implemented in the RCV system.

3. What are the procedures for disposing of the data at the end of the retention period? How long will the reports produced be kept? Where are the procedures documented?

Procedures for disposing hardcopies and electronic media are documented in the SORN.

4. Is the system using technologies in ways that the bureau/office has not previously employed (e.g., monitoring software, Smart Cards, Caller-ID)?

Yes, the RCV system will be using multiple AWS services to support operations and Security in the Cloud.

5. How does the use of this technology affect public/employee privacy?

This technology enhances privacy by allowing more secure protection than the previously employed solutions. AWS cloud enhances data security by using Identity and Access Management (IAM) that allows fine-grained access control, enforcing the least privilege policies with the role-based access and multi-factor authentication (MFA). AWS provides data encryption at rest and at transit using AWS Key Management Service (KMS) and SSL/TLS.

6. Will this system provide the capability to identify, locate, and monitor individuals? If yes, explain.

The RCV system records all user actions in an audit log which includes user id, type of action, date and time of action, and IP address of the computer, if available, but we do not monitor them (data is static, not dynamic) Using this information, when needed, the following can be determined:

- a. Who accessed the system?
- b. What function of the system was used?
- c. When was the system used?
- d. The IP address of the computer that was used to access the system.

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

Details are provided as part of the answer to the previous question. As mentioned to the previous answer, we do not monitor individuals.

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

The RCV system's audit log is accessible to only the following types of users:

- a. Users who are given direct access to the database (e.g., system administrators)
- b. Users who are given a specific access right to access the audit log.

9. Under which Privacy Act SORN does the system operate? Provide a number and name.

Federal Registry / Vol 65, No 184, page 57215-57222

10. If the system is being modified, will the Privacy Act SORN require amendment or revision? Explain.

Yes, SSS will modify the SORN to notify the public that the on-premises RCV system is now being hosted in an AWS Cloud.

Access to Data

1. Who will have access to the data in the system? (e.g., contractors, users, managers, system administrators, developers, others.)

Users, managers, system administrators, developers, and contractors will have access to the data.

2. How is access to the data by a user determined? Are criteria, procedures, controls, and responsibilities regarding access documented?

SSS has policies and procedures in place to grant users specific access to the system. Internal new users can request for access to the system, authorized user with appropriate access right will request appropriate user-role(s) for the user, another authorized user (different from the role requestor) with appropriate access right will approve/disapprove requested user-role(s).

3. Will users have access to all data on the system or will the user's access be restricted? Explain.

Access to data is controlled by user-roles and their associated access-rights which are implemented in the RCV system. Access is restricted by business function and not by individual data row or column in a database table.

4. What controls are in place to prevent the misuse (e.g., unauthorized browsing of data by those having access? (list processes and training materials.)

The RCV system implements the following controls to prevent the misuse of the system:

- a. All SSS employees and contractors go through the following training annually and also sign rules of behavior documents:
 - i. Cyber Awareness Challenge
 - ii. Insider Threat Rules of Behavior
 - iii. Privacy Act - PII Rules of Behavior
 - iv. General Information Technology Security Program Rules of Behavior
 - v. RCV System Rules of Behavior

- vi. Elevated User Agreement Rules of Behavior
- vii. Sensitive Data Nondisclosure Agreement
- b. Whenever users access the RCV system, they are warned that all of their actions are recorded and subject to monitoring.
- c. Upon request from an authorized SSS personnel, the system administrator has the ability to query the RCV system's audit log to find all actions performed by a user during a period of time.

5. Are contractors involved with the design and development of the system and will they be involved with the maintenance of the system? If yes, was Privacy Act contract clauses inserted in their contracts and other statutory and regulatory measures addressed?

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

6. Do other systems share data or have access to the data in the system? If yes, explain.

Yes, Power BI and the Central Registrant Processing Portal (CRPP) are using RCV's data. In addition, Enterprise Content Management System (ECM) is sharing data with RCV.

7. Who will be responsible for protecting the privacy rights of the public and employees affected by the interface?

Whoever has access to the RCV system and agencies participating in the use of the RCV system are responsible for protecting the privacy rights of the public and employees.

The Senior Agency Official for Privacy (SAOP) serves as the Agency's privacy officer responsible for ensuring all privacy regulations are met.

8. Will other agencies share data or have access to the data in this system (e.g. Federal, State, Local, and Others)?

Yes, other agencies provide data to the RCV system and receive data from the RCV system. Currently, there is no direct interface between the RCV system and other agencies.

9. How will the data be used by the other agency?

Other agencies use the data to determine eligibility to the benefits from the Federal government, employment with the Federal government, and other state-specific benefits. Data is also used to process an individual's request for a visa and to prosecute potential violators.

10. Who is responsible for assuring proper use of the data?

The system owner is responsible for assuring proper use of the data.

The Senior Agency Official for Privacy (SAOP) serves as the Agency's privacy officer responsible for ensuring all privacy regulations are met.

THE FOLLOWING OFFICIALS HAVE APPROVED THIS DOCUMENT

Chief information officer (CIO):

Jeffrey Steinlage Signature _____ Date _____

Chief Information Security Office (CISO):

Jonathan Kimball Signature _____ Date _____

Senior Agency Official for Privacy (SAOP):

Alma Cruz Signature _____ Date 4/17/2025

System Owner (SO):

Harry S. Kantor Signature _____ Date _____