Privacy Impact Assessment
for the

SELECTIVE SERVICE SYSTEM

August 2017

Contact Point:
CIO, Selective Service System

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

System Information

Name of System, Project or Program: RCV Modernization (RCV)
OMB Unique Identifier: (***if applicable***)

Contact Information

1. **Who is the person completing this document? (Name, title, organization, phone, email, address).**
   Prasad Perini
   Sr. Software Development Manager/Technical Lead/Architect
   ISHPI Information Technologies, Inc.
   115 SW Adams St, Suite 103
   Peoria, IL 61602
   (309) 999-4859
   Prasad.Perini@ishpi.net

2. **Who is the system owner? (Authorizing Official Name, title, organization, phone, email, address).**
   Scott Jones
   Chief Information Officer
   1515 Wilson Boulevard
   Arlington, VA 22209
   (703) 605-4128
   sjones@sss.gov

3. **Who is the system manager? (Name, title, organization, phone, email, address).**
   Anthony Clark
   Chief Information Security Officer
   1515 Wilson Boulevard
   Arlington, VA 22209
   (703) 605-4140
   aclark@sss.gov

4. **Who is the Information Systems Security Manager who reviewed this document? (ISSM Name, title, organization, phone, email, address).**
   Anthony Clark
   Information System Security Officer
   1515 Wilson Boulevard
   Arlington, VA 22209
   (703) 605-4128
   aclark@sss.gov

5. **Who is the Bureau Privacy Act Officer who reviewed this document? (Name, title, organization, phone, email, address).**

Scott Jones
Chief Information Officer
1515 Wilson Boulevard
Arlington, VA 22209
(703) 605-4128
sjones@sss.gov

6. **Who is the IT Reviewing Official? (CIO Name, title, organization, phone, email, address).**
   Adam Copp
   Associate Director of Operations
   1515 Wilson Boulevard
   Arlington, VA 22209
   (703) 605-4111
   acopp@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. Gender
   e. Suffix
   f. Social Security Number
   g. Date of Birth
   h. Street Address

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, Verification, and Correspondence (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:
   - SSS' public Web site: to support on-line registration, address update, and verification
   - SSS' Interactive Voice Response (IVR) system: to support registration and verification services over the phone
   - AAMVA's UNI: to receive data from Department of Motor Vehicles

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

2. **What are the sources of the 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:
      1. Mailing completed registration forms
      2. Mailing completed change of address forms
      3. Completing online registration using SSS public Web site
      4. Updating address information using SSS public Web site
      5. Registering with SSS using the IVR
      6. 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:
      1. Department Of Education
      2. States' Departments of Motor Vehicles
      3. U.S. Military Entrance Processing Command
      4. Military Academies
      5. U.S. Citizenship and Immigration Services
      6. Job Corps of the U.S. Department of Labor
      7. Alaska Permanent Fund
      8. Georgia Student Finance Commission
      9. 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:
      1. Defense Manpower Data Center of the Department of Defense

2. Department of Education
3. Department of Veterans Affairs
4. Job Corps of the U.S. Department of Labor
5. Office of Federal Investigation/Office of Personnel Management
6. Social Security Administration
7. U.S. Citizenship and Immigration Services
8. U.S. Coast Guard
9. U.S. Military Entrance Processing Command
10. 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:

1. State Department of Motor Vehicles
    1) Alabama
    2) Alaska
    3) Arizona
    4) Arkansas
    5) California
    6) Colorado
    7) Connecticut
    8) Delaware
    9) District of Columbia
    10) Florida
    11) Georgia
    12) Guam
    13) Hawaii
    14) Idaho
    15) Illinois
    16) Indiana
    17) Iowa
    18) Kansas
    19) Kentucky
    20) Louisiana
    21) Maine
    22) Maryland
    23) Massachusetts
    24) Michigan
    25) Minnesota
    26) Mississippi
    27) Missouri
    28) Montana
    29) Nebraska
    30) Nevada
    31) New Hampshire

32) New Jersey
33) New Mexico
34) New York
35) North Carolina
36) North Dakota
37) Ohio
38) Oklahoma
39) Oregon
40) Pennsylvania
41) Puerto Rico
42) Rhode Island
43) South Carolina
44) South Dakota
45) Tennessee
46) Texas
47) Utah
48) Vermont
49) Virgin Islands
50) Virginia
51) Washington
52) West Virginia
53) Wisconsin
54) Wyoming

2. Alaska Permanent Fund
3. Georgia Student Financial Commission

d. From what other third party sources will data be collected?

1. The following educational institutions send data to the RCV system requesting an individual's registration status:
    1) Kent State University
    2) Lakeland Community College
    3) Louisiana Community and Technical Colleges
    4) Louisiana State University
    5) Northwest State Community College
    6) Ohio State University
    7) Ohio University
    8) Owens Community College
    9) Sinclair Community College
    10) Terra Community College
    11) University of Akron
    12) University of Cincinnati
    13) University of Dayton
    14) University of Louisiana
    15) University of New Orleans
    16) University of Toledo
    17) Wright State University

18) Youngstown State University

2. Experian (for National Change Of Address service)

e. 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:

1. Gender
2. Name: First Name, Middle Name, Last Name, Suffix
3. Address
4. Social Security Account Number
5. Date of Birth

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 go 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.

1. Individuals submit changes using standard SSS forms
2. Individuals use SSS public Web site to update addresses
3. Individuals call SSS to update information
4. External sources that are listed above send information periodically
5. RCV sends information to Experian for address corrections

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 d?

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?**
   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.

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:
   1. Selective Service Number
   2. Social Security Account Number
   3. Document Locator Number
   4. Last Name
   5. Given Name
   6. Date of Birth
   7. Address
   8. PIN

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:
   1. List of individuals who are eligible for selective service to be used by the Department of Defense for marketing, recruiting, and drafting, when required
   2. List of individuals who are potential violators of the Military Selective Service Act to be used by the Depart of Justice to enforce the law
   3. 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 in more than one site, how will consistent use of the system and data be maintained in all sites?**
   The RCV system is implemented at a single site using one central database. 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 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 disposition 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)?**
   The RCV system records all user actions in an audit log which include: user id, type of action, date and time of action, and the IP address of the computer, if available.

5. **How does the use of this technology affect public/employee privacy?**
   It does not affect the privacy of the public. When users access the RCV system, they are notified that all actions are recorded. They can either agree and proceed to use the system, or cancel and exit the system.

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 include: user id, type of action, date and time of action, and IP address of the computer, if available. 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
   4. 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.

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

9. **Under which Privacy Act SORN does the system operate? Provide 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.**
    The SORN doesn't need to be updated specifically for the RCV system. There are no changes to the types of data that are collected, from where they are collected, or how they are used.

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. All personnel are security screened and vetted.

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:
   1. All SSS employees and contractors go through the following annually and sign rules of behavior documents:
      1) Cyber Awareness Challenge
      2) Identifying and Safe Guarding PII
      3) Phishing Awareness
      4) Insider Threat Awareness
      5) Privacy Act - PII Rules of Behavior
      6) General Information Technology Security Program Rules of Behavior
      7) RCV System Rules of Behavior

8) Elevated User Agreement Rules of Behavior

2. Whenever users access the RCV system, they are warned that all of their actions are recorded and subject to monitoring
3. 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
4. Currently the RCV system does not generate any usage monitoring reports

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.**
   Currently, there is no direct integration between the RCV system and any other system. Data is transmitted to and from other state and federal agencies that are listed under question #3 of the "Data in the system" section.

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 the protecting the privacy rights of the public and employees.

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 FOLLOWING OFFICIALS HAVE APPROVED THIS DOCUMENT

1. Information Systems Security Officer/Chief Information Security Officer

_____ (Signature) Date _____

2. Chief Information Officer/System Owner/ Privacy Act Officer

_____ (Signature) Date_____