



## **Privacy Impact Assessment (PIA)**

for the

### **Rehabilitation Services Administration Management Information System (RSA-MIS)**

**May 6, 2020**

**For PIA Certification Updates Only:** This PIA was reviewed on  by   
certifying the information contained here is valid and up to date.

### **Contact Point**

**Contact Person/Title:** Jack Johnson/IT Specialist

**Contact Email:** Jack.Johnson@ed.gov

### **System Owner**

**Name/Title:** Jack Johnson/IT Specialist

**Principal Office:** Office of Special Educational and Rehabilitative Services (OSERS)

Please submit completed Privacy Impact Assessments to the Privacy Office at  
[privacysafeguards@ed.gov](mailto:privacysafeguards@ed.gov)

Please complete this **Privacy Impact Assessment (PIA)** on how personally identifiable information (PII) is collected, stored, protected, shared, and managed electronically by your system. You may wish to consult with your ISSO in completing this document. **If a question does not apply to your system, please answer with N/A.**

## 1. Introduction

- 1.1. Describe the system including the name, acronym, and a brief description of the program or purpose for the system.

The Rehabilitation Services Administration (RSA) within the Office of Special Education and Rehabilitative Services (OSERS), operates the RSA Management Information System (RSA-MIS). This system collects information from RSA grantees regarding performance and expenditures under RSA grants to State agencies and other organizations. The RSA-MIS consists of three components. The first component is a web-based component which collects and disseminates performance and financial reports for RSA programs; data is collected through a variety of OMB-approved forms. No PII is collected in the first component. The second and third components relate to data collected and maintained related to the Case Service Report (RSA-911). The RSA-MIS is the system through which State Vocational Rehabilitation agencies upload quarterly RSA-911 files; this is the second component. The third component consists of a SQL Server database where RSA-911 data is maintained.

- 1.2. Describe the purpose for which the personally identifiable information (PII)<sup>1</sup> is collected, used, maintained or shared.

RSA-MIS maintains PII for program performance and accountability, and for research, monitoring, and evaluation purposes and is required by the Rehabilitation Act of 1973, as amended by title IV of the Workforce Innovation and Opportunity Act (WIOA), and title I of WIOA.

- 1.3. Is this a new system, or one that is currently in operation?

Currently Operating System

- 1.4. Is this PIA new, or is it updating a previous version?

---

<sup>1</sup> The term “personally identifiable information” refers to information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc. alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc. [OMB Circular A-130, page 33](#)

Updated PIA

1.5. Is the system operated by the agency or by a contractor?

Agency

1.5.1. If the system is operated by a contractor, does the contract or other acquisition-related documents include privacy requirements?

N/A

[Click here to select.](#)

## 2. Legal Authorities and Other Requirements

*If you are unsure of your legal authority, please contact your program attorney.*

2.1. What specific legal authorities and/or agreements permit and regulate the collection and use of data by the system? Please include name and citation of the authority.

The Rehabilitation Services Administration (RSA) was established by Congress as the principal federal agency authorized to carry out Titles I, III, VI and VII, as well as specified portions of Title V of the Rehabilitation Act of 1973, as amended by title IV of the Workforce Innovation and Opportunity Act (WIOA). RSA collects data in accordance with sections 101(a)(10), 106, and 607 of the Rehabilitation Act (29 U.S.C. §§ 721(a)(10), 726, and 7951).

### SORN

2.2. Is the information in this system retrieved by an individual's name or personal identifier such as a Social Security Number or other identification?

Yes

2.2.1. If the above answer is **YES**, this system will need to be covered by Privacy Act System of Records Notice(s) (SORN(s)).<sup>2</sup> Please provide the SORN name, number, Federal Register citation and link, or indicate that a SORN is in progress.

N/A

---

<sup>2</sup> A System of Records Notice (SORN) is a formal notice to the public that identifies the purpose for which PII is collected, from whom and what type of PII is collected, how the PII is shared externally (routine uses), and how to access and correct any PII maintained by ED. <https://connected.ed.gov/om/Documents/SORN-Process.pdf>

The Case Service Report (RSA-911) SORN (18-16-02) is pending publication in the Federal Register. Once published a link and citation will be inserted here.

**2.2.2.** If the above answer is **NO**, explain why a SORN was not necessary. For example, the information is not retrieved by an identifier, the information is not maintained in a system of records, or the information is not maintained by the Department, etc.

N/A

[Click here to enter text.](#)

### **Records Management**

**If you do not know your records schedule, please consult with your records liaison or send an email to [RMHelp@ed.gov](mailto:RMHelp@ed.gov)**

**2.3.** What is the records retention schedule approved by National Archives and Records Administration (NARA) for the records contained in this system? Please provide all relevant NARA schedule numbers and disposition instructions.

The Department shall submit a retention and disposition schedule that covers the records contained in this system to the National Archives and Records Administration (NARA) for review. The records will not be destroyed until such time as NARA approves said schedule.

**2.4.** Is the PII contained in this system disposed of appropriately, and in accordance with the timelines in the records disposition schedule?

Yes

### **3. Characterization and Use of Information**

#### **Collection**

**3.1.** List the specific PII elements (e.g., name, email, address, phone number, date of birth, Social Security, etc.) that the system collects, uses, disseminates, or maintains.

The personal information maintained includes, but is not limited to, the following: Social Security number (SSN), date of birth (DOB), gender, disability characteristics, demographic information including race and ethnicity, services and training received, health insurance, employment status, employment outcomes, earnings, ex-offender

status, other barriers to employment, and other program data elements included in the RSA-911.

- 3.2.** Does the system collect only the minimum amount required to achieve the purpose stated in Question 1.2?

Yes

- 3.3.** What are the sources of PII collected (e.g., individual, school, another agency, commercial sources, etc.)?

PII is collected from State VR agencies. The agencies collect PII directly from individuals who are participating in or have exited the VR program and the State Supported Employment (SE) program.

- 3.4.** How is the PII collected from the stated sources listed in Question 3.3 (e.g., paper form, web page, database, etc.)?

The PII is submitted as part of quarterly reports which are securely uploaded to the RSA-MIS by the State VR agencies.

- 3.5.** How is the PII validated or confirmed to ensure the integrity of the information collected?<sup>3</sup> Is there a frequency at which there are continuous checks to ensure the PII remains valid and accurate?

When the file is submitted to RSA, RSA runs the file through a series of logic-based edit checks. Any errors identified by these checks are then provided to the agency, via email. These errors do not include PII.

#### Use

- 3.6.** Describe how the PII is used to achieve the purpose stated in Question 1.2 above.

RSA collects PII for performance accountability provisions in title I of WIOA., WIOA requires that RSA report on the primary indicators of performance, established in section 116, based on characteristics of the VR program participants being served, including but not limited to sex, age, and race/ethnicity. The RSA-911 data elements collected by VR agencies and reported to RSA allow for this breakdown.

---

<sup>3</sup> Examples include restricted form filling, account verification, editing and validating information as it's collected, and communication with the individual whose information it is.

Once collected from state VR agencies, the data is also shared with the Social Security Administration (SSA) pursuant to Federal requirements, to monitor and evaluate programs serving individuals with disabilities. Sharing information enhances the program research and evaluation capabilities of both agencies because much of this research can be conducted only by exchanging data with each other. Under the established memorandum of understanding, SSA will match RSA's annual file of RSA-911 data to SSA program records to create a matched data set (stripped of certain personal identifiers) that will be used for authorized research projects.

**3.7.** Is the system using PII for testing/researching new applications or information systems prior to deployment or for training employees?

No

**3.7.1.** If the above answer is **YES**, what controls are in place to minimize the risk and protect the data?

N/A

### **Social Security Numbers**

*It is the Department's Policy that, in order to collect Social Security Numbers, the System Owner must state the collection is: 1) authorized by law, 2) necessary for an agency purpose, and 3) there is no reasonable alternative.*

**3.8.** Does the system collect Social Security Numbers? Note that if the system maintains Social Security Numbers but does not explicitly collect them, answer 3.8.1 to address the purpose for maintaining them.

Yes

**3.8.1.** If the above answer is **YES**, explain the purpose for its collection, and how the SSN will be used.

N/A

The SSN is needed to share data with the Social Security Administration which merges SSI (Social Security Insurance) and SSDI (Social Security Disability Insurance) information based on the SSN. The SSN is necessary for confirming the identity of the individual.

**3.8.2.** Specify any alternatives considered in the collection of SSNs and why the alternatives were not selected.

N/A

The collection of SSN is required to satisfy statutory requirements related to data sharing with SSA. No other alternative can be considered.

#### **4. Notice**

**4.1.** How does the system provide individuals with notice about the collection of PII prior to its collection (e.g., direct notice, such as a Privacy Act Statement (if applicable) or public notice, such as a SORN, PIA,)? If notice is not provided, explain why not.

The Department does not provide direct notice to individuals regarding the collection of their information. State VR agencies are required to inform individuals being served by their programs that their information is being collected and provided to the Department.

Public notice is provided through the publication of this PIA and the SORN referenced in 2.2.1.

**4.2.** Provide the text of the notice or the link to the webpage where the notice is posted if notice is provided other than by SORN or PIA.

N/A

**4.3.** What opportunities are available for individuals to consent to uses (including new uses of previously collected PII), decline to provide PII, or opt out of the project?

Individuals with disabilities, who are engaged in the VR program, at the State-level are not required to provide PII, including the SSN, to the State VR agency. In other words, they may opt out of sharing this information.

**4.4.** Is the notice referenced in Question 4.1 reviewed and revised when there are changes in the practice, policy, or activities that affect the PII and privacy to ensure that individuals are aware of and can consent to, where feasible, these changes?

Yes

#### **5. Information Sharing and Disclosures**

## Internal

5.1. Will PII be shared internally with other ED principal offices? If the answer is **NO**, please skip to Question 5.4.

No

5.2. What PII will be shared and with whom?

N/A

5.3. What is the purpose for sharing the specified PII with the specified internal organizations?

N/A

## External

5.4. Will the PII contained in the system be shared with external entities (e.g. another agency, school district, the public, etc.)? If the answer is **NO**, please skip to Question 6.1.

Yes

5.5. What PII will be shared and with whom? List programmatic disclosures only.<sup>4</sup>

**Note: If you are sharing Social Security Numbers externally, please specify to whom and for what purpose.**

N/A

The PII RSA has is shared with SSA for data-matching purposes with SSA records.

5.6. What is the purpose for sharing the PII with the specified external entities?

N/A

RSA's information is shared with SSA to merge Social Security Insurance (SSI) and Social Security Disability Insurance (SSDI) with the records provided to the Department by state VR agencies. The SSN is necessary for confirming the identity of the individual.

---

<sup>4</sup> If this information is covered by Privacy Act System of Records Notice (SORN) please list only relevant programmatic disclosures listed under the Routine Uses section.

5.7. Is the sharing with the external entities authorized?

N/A

Yes

5.8. Is the system able to provide and retain an account of any disclosures made and make it available upon request?

N/A

Yes

5.9. How is the PII shared with the external entity (e.g. email, computer match, encrypted line, etc.)?

N/A

An annual file is hand delivered to SSA.

5.10. Is the sharing pursuant to a Computer Matching Agreement (CMA), Memorandum of Understanding (MOU), or other type of approved sharing agreement with another agency?

N/A

Yes

5.11. Does the project place limitation on re-disclosure?

N/A

Yes

## 6. Redress

6.1. What are the procedures that allow individuals to access their own information?

Individuals may request information related to their record(s) in the RSA-911 databases by reaching out to the system owner by reaching out to the system owner as detailed in the SORN.

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

Individuals may correct inaccurate or erroneous information in the RSA-911 databases by reaching out to the system owner as detailed in the SORN.

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

Individuals are notified in the published SORN for the procedures for correcting their information.

## 7. Safeguards

*If you are unsure which safeguards will apply, please consult with your [ISSO](#).*

7.1. Does the principal office work with their CSO/ISSO to build privacy & security into the system and build privacy extensions to the extent feasible?

Yes

7.2. Is an Authority to Operate (ATO) required?

Yes

7.3. Under [NIST FIPS Pub. 199](#), what is the security categorization of the system: **Low, Moderate, or High?**

N/A

Moderate

7.4. What administrative, technical, and physical safeguards are in place to protect the information?

System Security Plan details the security requirements and describes the security controls that are in place to meet those requirements. Additional storage and safeguards information is contained in the applicable System of Records Notice.

RSA employees who can access the database are controlled and have approved Privileged User Agreements in place and the necessary security clearance levels to do so. Access to this system will require a unique user identification as well as a password to enter the system. Users will be required to change their passwords periodically, and they will not be allowed to repeat old passwords. Any individual attempting to log on who fails is locked out of the system after three attempts. Access after that time requires intervention by the system manager.

The computer system employed by the Department offers a high degree of resistance to tampering and circumvention. This security system limits data access to Department and contract staff on a “need to know” basis and controls individual users' ability to access and alter records within the system.

The location of the server includes safeguards and firewalls, including the physical security of the server room. In addition, the server is located in a secure room, with limited access only through a special pass. Further, all physical access to the site where the server is maintained is controlled and monitored by security personnel who check each individual entering the building for his or her employee or visitor badge. In addition to these controls, computers are not left on and unattended when users access the database, and sensitive information is placed out of sight if visitors are present.

Shared output does not contain sensitive information. Aggregated data cannot be used to identify individuals. In addition, the following guidelines and procedures have been implemented for protecting sensitive data and resources in this system: Users must use two-factor authentication to access the Department of Education network and Users are not permitted to copy files to portable electronic media such as compact discs or USB drives.

7.5. Is the information in the system appropriately secured in accordance with the IT security requirements and procedures as required by Federal law and policy?

Yes

7.6. Has a risk assessment been conducted where appropriate security controls to protect against that risk have been identified and implemented?

Yes

7.7. Please describe any monitoring, testing or evaluation conducted on a regular basis to ensure the security controls continue to work properly at safeguarding the PII.

The RSA-911 database is scanned weekly and the information is provided to various application owners. There is a mature patching process in which patches are downloaded from vendor supported repositories and reviewed by administrators before scheduling for application on a regular schedule. Patches are applied first in non-production environments and allowed to operate for a week as a test before application to production environments.

Additionally RSA-MIS is required to be granted an Authorization to Operate (ATO) on a tri-annual basis. This process includes a rigorous assessment of security controls, a plan of action and milestones to remediate any deficiencies, and a continuous monitoring program between the full scope assessments.

## **8. Auditing and Accountability**

- 8.1.** How does the system owner assess and ensure that the PII is used in accordance with stated practices in this PIA?

The RSA-MIS system owner does not have access to the PII maintained in the SQL Server database but is responsible for maintaining all required security and privacy documentation to ensure PII is handled appropriately. Other RSA staff, with approved PUAs, access records and prepare files for sharing with SSA, as appropriate. The Data Collection and Analysis Unit Chief approves all data-sharing of RSA-911 data, including the SSA files and those files that do not contain any PII or aggregated data.

- 8.2.** Does the system owner continuously monitor and audit the privacy controls to ensure effective implementation?

Yes

- 8.3.** What are the privacy risks associated with this system and how are those risks mitigated?

There is a risk that PII, including the SSN, could be disclosed to an unauthorized person. This risk is mitigated by encrypting the PII when it is stored in the database with a password protected key. It is further mitigated by only permitting two RSA staff to have access to the database server that contains the data for the system. These staff have the necessary PUAs in place that substantiate their security clearance.