Privacy Impact Assessment (PIA)

for the

National Clearinghouse for Rehabilitation Training Materials (NCRTM)

January 6, 2021

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

Contact Point

Contact Person/Title: Kristen Rhinehart-Fernandez
Contact Email: Kristen.Rhinehart@ed.gov

System Owner

Name/Title: Kristen Rhinehart-Fernandez
Principal Office: Office of Special Education Rehabilitative Services (OSERS)

Please submit completed Privacy Impact Assessments to the Privacy Office at 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), a division of the U.S. Department of Education's (Department's) Office of Special Education and Rehabilitative Services, satisfies Section 15 of the Rehabilitation Act of 1973 (29 U.S.C. § 701) through the National Clearinghouse of Rehabilitation Training Materials (NCRTM). NCRTM, a public-facing website and portal with a backend database visible only to system administrators, facilitates the sharing of information and resources for individuals with disabilities and their families, vocational rehabilitation (VR) personnel and professionals, relevant public and private agencies, and the general public. NCRTM contains training and technical assistance materials, research, practices supported by promising evidence, and curriculum designed to help individuals with disabilities eligible for VR services, including youth with disabilities, secure competitive integrated employment, as well as enable state VR agency personnel and other professionals in the VR field to manage available resources, improve effective service delivery, and increase the number and quality of employment outcomes for individuals with disabilities.

Primary users of NCRTM include RSA staff, VR administrators, Federal partners, discretionary grantees, rehabilitation educators and trainers, businesses, VR counselors and paraprofessionals, and other workforce system partners. Other workforce system partners are organizations and entities that the Department coordinates and collaborates with to ensure that individuals with disabilities have every opportunity to obtain competitive integrated employment. Examples of national organizations may include but are not limited to the Council of State Administrators of Vocational Rehabilitation (CSAVR), National Council on Rehabilitation Education, National Council of State Agencies for the Blind, and Consortia of Administrators for Native American Rehabilitation.

The purpose of the NCRTM portal is for RSA grantees to upload documents that were developed with RSA funding, and for organizations/individuals to submit materials in subsequent sessions without reentering the required user information. When a grantee creates an account, the grantee can upload materials to the portal. The uploaded materials will be directed to the responsible RSA project officer for review per RSA grantee requirements. Users who have created an NCRTM account can check on the status of a submitted material or upload new materials to the NCRTM. Information is collected from users who register for an account or submit materials

(with or without registering for an account) to be considered for inclusion in the NCRTM library. To create an account, users are required to provide name, job title, organization, work email address, phone number, work address, username, and password. Registered users submitting materials related to grants also submit a PR/Award number (a unique Department-specified identifying number that is assigned to each application/grant award). Users with accounts who are logged into the system can access and update the information by selecting "Manage Profile." The system provides two-factor authentication to safeguard access to user information. Users do not need to register for an account to submit materials through the portal. The primary difference between registered and unregistered users is the ability for registered users to view the status of submitted materials. To submit materials, unregistered users provide name, job title, work email address, organization, work address, and work phone number.

System administrators, who are either Federal employees or contractors, can also log into the system using a username and password to access user information. System administrators periodically deactivate old accounts or, in rare cases, update account user contact information at users' request or obtain users' work email addresses so they can email them questions about their submissions.

1.2. Describe the purpose for which the personally identifiable information (PII)[1] is collected, used, maintained or shared.

Grantees: The purpose of the NCRTM portal is for RSA grantees to upload documents that were developed with RSA funding, and for organizations/individuals to submit materials in subsequent sessions without reentering the required user information. Information is collected from users who register for an account or submit materials (with or without registering for an account) to be considered for inclusion in the NCRTM library. Users do not need to register for an account to submit materials through the portal. The primary difference between registered and unregistered users is the ability for registered users to view the status of submitted materials. In addition, the NCRTM librarian (a system administrator) uses the information collected to contact individuals if there are questions about or issues with the materials they have submitted.

System Administrators: Information is collected to track access provided to system administrators for the purpose of reviewing submissions.

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

[1] 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

Currently Operating System

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

Updated PIA

The PIA is being updated as part of the required biennial review.

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

Contractor

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

Yes

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.

Legislative Authority: Section 15 of the Rehabilitation Act of 1973 (29 U.S.C. § 701), as amended by the Workforce Innovation and Opportunity Act (WIOA). SEC. 15. (a) The Secretary of Education shall establish a central clearinghouse for information and resource availability for individuals with disabilities which shall provide information and data. The clearinghouse shall also provide any other relevant information and data which the Secretary of Education considers appropriate. (b) The Commissioner may assist the Secretary of Education to develop within the Department of Education a coordinated system of information and data retrieval, which will have the capacity and responsibility to provide information regarding the information and data referred to in subsection (a) of this section to the Congress, public and private agencies and organizations, individuals with disabilities and their families, professionals in fields serving such individuals, and the general public. (c) The office established to carry out the provisions of this section shall be known as the ‘‘Office of Information and Resources for Individuals with Disabilities’’. (d) There are authorized to be appropriated to carry out this section such sums as may be necessary. [29 U.S.C. 712]

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?

No

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)).[2] Please provide the SORN name, number, Federal Register citation and link, or indicate that a SORN is in progress.

☑ N/A

Click here to enter text.

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

The information is not retrieved by an identifier.

Records Management

If you do not know your records schedule, please consult with your records liaison or send an email to 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.

NCRTM manages records in accordance with the Department: https://www2.ed.gov/notices/records-management/index.html (schedule locator number 254: Grant administration and management files, disposition N1-441-11-001), section E final grant products, routine products and products determined to be of "historical significance." The NCRTM is the only repository that exists in the Vocational Rehabilitation field. Products on the NCRTM are submitted by grantees and the field for informational purposes or to fulfill grant performance requirements which are of enduring value. In accordance with the Statute that mandates the NCRTM, products contained on the NCRTM are to be retained permanently. The program office will determine if there are any products that are out of date or no longer relevant due to changes in the law or program regulations and will remove those products from the NCRTM, as necessary.

[2] 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

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

Yes, if products are determined to be no longer relevant, they will be removed from the NCRTM.

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 following information is collected from grantees (* indicates required fields):

- Name*
- Job title*
- Organization*
- Organization website
- Work email address*
- Phone number*
- Work address (street address, city, state, zip code*)
- PR/Award Number
- Username (only for individuals who register for an account)
- Password (only for individuals who register for an account)

The following information is collected from system administrators:

- Name
- Work Email address
- Username
- Password

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

Yes

The system collects grantee name, job title, organization, work email address, work phone number, work address, username, and password which is the minimum necessary to establish an account for inclusion in the NCRTM library. This information is needed

to vet account creation requests to ensure access is being provided to individuals that have a genuine need and in addition to allow for contacting grantees, as necessary.

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

The sources of the PII can be any member of the public that submits information to the NCRTM. Generally, this includes discretionary grantees (i.e., institutions of higher education, minority entities and Indian tribes, State and public or non-profit agencies and organizations) and formula grantees (i.e., State VR agencies) funded by the Department, and through partnerships with other Federal and non-Federal agencies that assist State and other agencies in providing VR and other services to individuals with disabilities. In addition, for internal administration, sources of PII include Federal employees and contractors.

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

Grantees: The information is collected via web forms for individuals who submit materials to the NCRTM for RSA's consideration.

System Administrators: For new system administrators, the information is collected and entered into the system by an existing system administrator.

3.5. How is the PII validated or confirmed to ensure the integrity of the information collected?[3] Is there a frequency at which there are continuous checks to ensure the PII remains valid and accurate?

The information is validated using an automated process to confirm that the data entered meet the following specific requirements:

- Name* – Must include text.
- Job Title* – Must include text.
- Organization* – Must include alphanumeric characters.
- Organization Website – Must include http:// or https:// in the URL.
- Work email address* – Must include @.com, @.net, etc.
- Work Phone number* – Must be in ###-###-#### format.
- Work address, City, State, Zip code – Zip code must be in ##### format.

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

- PR/Award Number – Must be in the following format: (H###A######) H, followed by the Assistance Listing Number (ASLN) (i.e., 315C), followed by the Federal Fiscal Year, followed by the application number (i.e., 1, 2, 3, etc.).

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

The information is collected in order to ensure individuals who need access for submission or create accounts are vetted appropriately to ensure access is being provided to individuals that have a genuine need prior to accepting a submission or creating an account for access. In addition, the NCRTM librarian uses the information to follow up with individuals if there is a question about their submissions. For example, if the material is not accessible to people with disabilities, if they forgot to attach a file (i.e., the material), or if they forgot to add topics for indexing in the library. Accounts do not require individuals to submit information each time, which provides a degree of convenience when users submit materials during multiple sessions. The account also allows individuals to view whether materials submitted have been approved or denied by the assigned RSA project officer for inclusion in the NCRTM.

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

Click here to enter text.

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.

No

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

☑ N/A

Click here to enter text.

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

☑ N/A

Click here to enter text.

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.

A privacy notice, as shown below, is posted on the collection website.

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

Authorities: The following authorities authorize the collection of this information: Section 15 of the Rehabilitation Act of 1973 (29 U.S.C. § 701), as amended by the Workforce Innovation and Opportunity Act (WIOA). SEC. 15.

Information Collected: Name*, job title*, organization*, organization website, work email address*, work phone number*, work address, PR/Award Number.

NOTE: * denotes information that is required.

Purpose: The purpose of collecting this information is to: (1) allow Department employees and contractors to utilize the system as part of normal system/registration and access activities, and (2) allow the Department to contact individuals who provide information to the NCRTM portal if there are questions about or issues with the materials they have submitted.

Disclosures: The information will not be disclosed outside of the Office of Finance and Operations.

Consequences of Failure to Provide information: The purpose of the NCRTM portal is for RSA grantees to upload documents funded by RSA, and for organizations/individuals to submit multiple materials. Failure to provide required information or forego creating an account may result in not having the ability to check on the status of a submitted material or upload new materials to the NCRTM.

Additional information about this system can be found in the Privacy Impact Assessment.

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?

Providing the information is completely voluntary. Individuals can contact NCRTM if they do not wish to complete the form and still want to submit materials and bypass providing the 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

Click here to enter text.

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

☑ N/A

Click here to enter text.

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.

No

5.5. What PII will be shared and with whom? List programmatic disclosures only.[4]
Note: If you are sharing Social Security Numbers externally, please specify to whom and for what purpose.

☑ N/A

Click here to enter text.

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

☑ N/A

Click here to enter text.

5.7. Is the sharing with the external entities authorized?

☑ N/A

Click here to select.

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

☑ N/A

No

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

☑ N/A

Click here to enter text.

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

[4] 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.

Click here to select.

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

☑ N/A

Click here to select.

6. Redress

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

Individuals can either log into the NCRTM and use its Manage Profile feature or email a request to the NCRTM librarian at NCRTM@neweditions.net.

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

Individuals can either log into the NCRTM and use its Manage Profile feature or email a request to the NCRTM librarian at NCRTM@neweditions.net to change correct inaccurate or erroneous information.

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

The NCRTM email address is presented on the Contact Us page of the website.

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

Low

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

New Editions Consulting, Inc. maintains the NCRTM and Microsoft Azure hosts the NCRTM for the Department. New Editions developed policies, procedures, and protocols for physical and environmental protection of New Editions owned and supported information systems and the PII contained within them. Protections include: video monitored reception area; a visitor log; elevator keys to access the floor office during non-business hours; and the requirement that users log off their computers when they are not at their desks. These safeguards help to prohibit unauthorized individuals from gaining access to the system and the information contained within it while at the New Editions office.

Microsoft Azure enforces physical access authorizations for all physical access points to Azure datacenters using 24x7 staffing, alarms, video surveillance, multifactor authentication, and man-trap portal devices. Physical access to a Microsoft Azure datacenter must be approved by the Datacenter Management (DCM) team using its datacenter access tool. Access levels are assigned in the tool to either a user's Microsoft issued badge or a temporary access badge that is assigned at the datacenter by the Control Room Supervisor (CRS). Access levels are approved by the DCM team. In addition to credentials assigned to physical badges, some areas of the datacenter require enrollment of the user's biometric data (hand geometry or fingerprint). Additionally, when access is no longer required, datacenter security officers or management manually request the termination of access.

Additionally, annually, and as warranted, staff who have access to the NCRTM application are provided the Department Security and Privacy Awareness training. The training includes information on what constitutes PII and Sensitive PII (SPII) and how to maintain, protect, and safeguard it, as well as the steps to perform if PII/SPII is accessed without authorization.

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.

There are three different types of vulnerability scans performed on a regular basis to safeguard PII and the NCRTM system. First, application scans are conducted every month by the Department's Vulnerability and Management (V&M) Team using WebInspect. Second, database scans are conducted monthly by New Editions Consulting, Inc. using Azure Vulnerability Assessment. Third, server scans are conducted regularly by Microsoft using proprietary tools.

Results are uploaded to the Cyber Security Assessment and Management (CSAM) system, the Department's official repository of information systems, which provides the information assurance and program officials with a web-based secure network capability to assess, document, manage, and report on the status of IT for security authorization processes in the risk management framework in accordance with the Federal Information Security Modernization Act of 2014 (FISMA). If any vulnerabilities are discovered, they are remediated within the specified timeframe based on severity. The system requires annual audits of security artifacts and controls to ensure proper National Institute of Standards and Technology (NIST) security and privacy controls are documented and operating as intended.

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?

Federal employees and contractor staff are provided security and privacy awareness and training as indicated in section 7.4. They are made aware that the PII contained within NCRTM is for collection and maintenance and not to be distributed, exported, or printed. In addition, Federal employees and contractor staff sign rules of behavior regarding their use of the NCRTM and information contained within the system. Monthly vulnerably scans and system audits are conducted to reduce the risk of outside threats obtaining the PII.

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?

Privacy risks associated with NCETM include unencrypted data being transmitted, lost, stolen, or compromised. Data breaches involving PII are potentially harmful to both individuals and organizations. Individual harm may include identity theft, embarrassment, or financial loss. Organizational harm may include a loss of public trust, legal liability, or remediation costs.

RSA and contractor staff, systems and processes select and implement NIST Special Publication 800-53 controls, which include administrative, technical, and physical controls. These controls are in place to ensure the integrity, availability, confidentiality, accuracy, and relevancy of the data and to mitigate privacy risks. The risks are mitigated by granting access to only authorized individuals based on their respective position and on a need-to-know basis, limiting users to those who are screened, utilizing least privilege principles, and encrypting data in transmission.