Privacy Impact Assessment (PIA)
for the

National Clearinghouse for Rehabilitation Training Materials (NCRTM)
December 18, 2023

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: Diandrea Bailey/Information System Owner
Contact Email: Diandrea.Bailey@ed.gov

System Owner

Name/Title: Diandrea Bailey/Information System Owner
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) Office of Special Education and Rehabilitative Services is responsible for satisfying Section 15 of the Rehabilitation Act of 1973[1], as amended (29 U.S.C. § 701). RSA funds the NCRTM to meet the Sec. 15 requirements. The NCRTM facilitates the sharing of information and resource availability for individuals with disabilities and their families, Vocational Rehabilitation (VR) personnel, as well as professionals in the field of VR, relevant public and private agencies, and the general public. The NCRTM contains training and technical assistance materials, research, practices supported by promising evidence, and a 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 improve service delivery and increase the number and quality of employment outcomes for individuals with disabilities.

To meet the statutory requirement described above, the NCRTM receives, catalogs, and disseminates materials (e.g., informational documents, website links, multimedia files) developed by formula and discretionary grantees funded by the Department. Grantees may include State and public or nonprofit agencies and organizations including American Indian tribes and Institutions of Higher Education (IHEs). Organizations and individuals may also submit materials they deem relevant for the NCRTM via an online library submission form. Submitters are required to provide their name, organization, work email address, and PR/Award number, if applicable. The information is solely used to follow up with the submitter in case there are any questions about their submission.

Grantees are required per the Notice Inviting Applications (NIA) that funded the award(s) to submit materials developed with grant funds to the NCRTM. An NIA announces and invites grant application submissions for one or more competitions and contains important information such as application requirements. When grantees submit their materials, the PR/Award Number must be included, which is a unique identifier

[1] The Rehabilitation Act of 1973 as amended by WIOA (PDF). Section 15 is located on page 26.

that is generated through G5 when applications are submitted to Grants.gov (example: H160D210001).

NCRTM also maintains a newsletter and can send users notifications when materials are uploaded to the system. Users can sign up for these mailing lists through a web form that collects name, email address, and organization. NCRTM also conducts surveys through the website that assess website visitors' satisfaction with their experiences navigating the website. No PII is collected through the survey.

1.2. Describe the purpose for which the personally identifiable information (PII)[2] is collected, used, maintained, or shared.

- Submitters: Information is collected from users who submit materials to be considered for inclusion in the NCRTM library. System administrators use the information collected to contact individuals if there are questions about or issues with the materials they have submitted.
    - Grantees are required per the Notice Inviting Applications that funded the award(s) to submit materials developed with grant funds to the NCRTM. An NIA announces and invites grant application submissions for one or more competitions and contains important information such as application requirements. When grantees submit their materials, the PR/Award Number must be included, which is a unique identifier that is generated through G5 when applications are submitted to Grants.gov (example: H160D210001). Grantees may include State and public or nonprofit agencies and organizations including American Indian tribes and IHEs.
    - Organizations and individuals may also submit materials they deem relevant for the NCRTM via an online library submission form. Submitters are required to provide their name, work email address, organization, and PR/Award number, if applicable. The information is solely used to follow up with the submitter in case there are any questions about their submission.

- System Administrators: Information is collected to provide and track access provided to system administrators to review submissions.
- Newsletter: Individuals subscribing to the NCRTM newsletter submit information to facilitate the newsletter being sent to them.

[2] 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

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?

Updated PIA

The PIA is being updated to reflect technical changes to the NCRTM system environment. NCRTM migrated from a .NET-based application to a Content Management System (Drupal 9). The major functional objective for this transition is to obtain a more configurable application with improved search capabilities, a modernized appearance that adheres to the Department's style guide for websites, and increased responsiveness (for mobile users) to adhere to the 21st Century Integrated Digital Experience Act (IDEA), which aims to improve the digital experience for government customers accessing Federal public websites.

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?

☐ N/A

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 that 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)).[3] Please provide the SORN name, number, Federal Register citation, and link, or indicate that a SORN is in progress.

☑ N/A

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

Information is not retrieved by a name or unique 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.

[3] 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

NCRTM manages records in accordance with:

- Grant Case Files: General Records Schedule (GRS) 1.2, item 020: Temporary. Destroy 10 years after final action is taken on file, but longer retention is authorized if required for business use.
- Final Grant products or deliverables, not historically significant: GRS 1.2, item 030: Temporary. Destroy when business use ceases.

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 following information is collected from grantees and other submitters:

- Name
- Organization
- Work email address
- PR/award number, if applicable

The following information is collected from individuals signing up for the newsletter:

- Name
- Email address
- Organization

The following information is collected for 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 name, organization, PR/award number, and work email address which is the minimum information necessary to contact material submitters if required. For individuals to receive the newsletter, name, email address, and organization are the minimum amount of information required. Name, email address, username, and password constitute the minimum information required for maintaining user accounts for system administrators. Failure to provide the required information may result in the inability to upload materials to the NCRTM or receive the NCRTM newsletter.

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

- Submitters: The source of the PII can be any member of the public that submits information to the NCRTM. Generally, this includes discretionary grantees (i.e., IHEs, minority entities, 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.
- Newsletter: Sources of PII for the newsletter are any member of the public that signs up to receive the newsletter.
- System Administrators: For system administration, sources of PII include Department 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.)?

- Submitters: The information is collected via a web form for individuals who submit materials to the NCRTM for RSA's consideration.
- Newsletter: Information is collected via a web form for individuals who wish to receive the newsletter.
- 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?[4] 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 meets the following specific requirements:

- Name – Must include text.
- Organization – Must include alphanumeric characters.
- Email address – Must include @.com, @.net, etc.
- PR/Award Number (if applicable) – 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.).

Use

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

NCRTM system administrators use the information provided to follow up with individuals if there is a question about their submissions, e.g. 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. In addition, individuals subscribing to the NCRTM newsletter submit information to facilitate the newsletter being sent to them.

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.

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

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

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

☑ N/A

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, or PIA)? If notice is not provided, explain why not.

A privacy notice, as shown in 4.2, 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, organization, work email address, and PR/Award Number, if applicable.

Purpose: The purpose of collecting this information is to allow the Department to contact individuals who provide information to the NCRTM portal if there are questions about or issues with the materials submitted. In addition, individuals subscribing to the NCRTM newsletter submit information to facilitate the newsletter being sent to them.

Disclosures: Information may be disclosed to Department contractors in the course of normal business. The Department does not otherwise anticipate further disclosing of the information provided.

Consequences of Failure to Provide Information: The purpose of the NCRTM portal is for RSA grantees to upload materials funded by RSA, and for organizations/individuals to submit materials or sign up for the newsletter. Failure to provide the required information may result in the inability to upload materials to the NCRTM or receive the newsletter.

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?

The provision of information by material submitters is voluntary. Individuals may contact NCRTM if they do not wish to complete the form and still want to submit materials and bypass providing the information.

A newsletter subscription is voluntary, but the information is required to receive the newsletter.

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.

No

5.5. What PII will be shared and with whom? List programmatic disclosures only.[5]
Note: If you are sharing Social Security Numbers externally, please specify to whom and for what purpose.

☑ N/A

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

☑ N/A

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

Click here to select.

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

☑ N/A

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

[5] 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 email a request to NCRTM at NCRTM@neweditions.net.

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

Individuals can email a request to NCRTM at NCRTM@neweditions.net to change or 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 at the top of the materials submission form.

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. (New Editions) maintains NCRTM, which is hosted on Microsoft Azure. 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. Physical protections include a 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 mitigate the risk of unauthorized individuals gaining access to the system and the information contained within it.

Microsoft Azure enforces authorizations for all physical access points to Azure data centers using 24/7 staffing, alarms, video surveillance, multifactor authentication, and man-trap portal devices. Physical access to a Microsoft Azure data center must be approved by the Datacenter Management (DCM) team using its data center 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 data center 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 data center require enrollment of the user's biometric data (hand geometry or fingerprint). Additionally, when access is no longer required, data center 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 information assurance and program officials with a web-based secure network capability to assess, document, manage and report on the status of information technology (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?

The system owner works with the Department's Privacy Office to complete both PTA and PIA forms and ensure both are accurate and updated as required. The system owner also completes the Department Risk Management Framework process and participates in the Department's Ongoing Security Authorization (OSA) program to maintain an ATO. Under this process, an independent assessor assesses a variety of controls each quarter to ensure the system and the data residing within are appropriately secured and protected. The system owner works with contractors to ensure the system is being used appropriately and in accordance with the practices detailed in this document. 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 is 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.

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 NCRTM include unencrypted data being transmitted, lost, stolen, or compromised. Data breaches involving PII are potentially hazardous 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.

The risks are mitigated by the above-mentioned safeguards, limiting access to only those with a legitimate need to know, and working closely with the security and privacy staff at the Department. To further mitigate this risk, the following safeguards have been implemented:

- Monthly vulnerability scans
- Annual contingency plan test
- Annual or ongoing security assessments

Risks are also mitigated by updating security patches per the patch scheduling and updating devices operating software, amongst other software. System patching is performed monthly, and scans are run on the production environment each month in support of the monthly patching cycle.