

CJG



ADMINISTRATIVE OFFICE  
45 SOUTH FRUIT STREET  
CONCORD, NH 03301-4857



5C

GEORGE N. COPADIS, COMMISSIONER

RICHARD J. LAVERS, DEPUTY COMMISSIONER

September 11, 2025

Her Excellency, Governor Kelly A. Ayotte  
and the Honorable Council  
State House  
Concord, NH 03301

**REQUESTED ACTION**

To authorize New Hampshire Employment Security (NHES) to enter into an amendment to the **sole source no cost** Integrity Data Hub (IDH) Participation Agreement Version 6.0, with the National Association for State Workforce Agencies' (NASWA's) Center for Employment Security Education and Research, Inc. (CESER), located at 444 N. Capitol Street, NW Suite 300, Washington, DC, from the date of Governor and Council approval through September 30, 2027. NHES received G & C approval to enter into IDH Participation Agreement Version 6.0 on October 16, 2024 (Item #44).

**EXPLANATION**

In order to prevent and address fraud in the Unemployment Insurance (UI) System, the National Association of State Workforce Agencies (NASWA) has worked with the United States Department of Labor (USDOL) to develop an Integrity Data Center (IDC) and Integrity Data Hub (IDH). These resources were created to facilitate cross-matching of suspicious UI claims information by and between the States. NASWA, through CESER, has a Cooperative Agreement with USDOL to operate the IDC and IDH. States must enter into a "Participation Agreement" to engage in the IDH data exchange network.

NHES is authorized by RSA 282-A:118, VIII to participate in the IDH, and first received Governor & Council approval to enter into IDH Participation Agreement Version 5.0 on October 13, 2021 (Item #55). As noted above, NHES received G & C approval to enter into IDH Participation Agreement Version 6.0 on October 16, 2024 (Item #44), which added new functionality to the data sharing, and includes a directory of fraudulent employers.

In order to capitalize on existing federal resources and promote sustainability, the agreement was expanded to include provisions for NASWA/CESER to be designated as an agent of the States in specific transactions with the US Treasury, Bureau of Fiscal Service (Fiscal Service). NASWA has worked closely with the Fiscal Service to obtain access to new data sources and to provide alternative capabilities that currently exist within IDH, specifically the Identity Verification (IDV) and Bank Account Verification (BAV) solutions, through the Fiscal Service. NASWA/CESER's designation as an agent of the States for these specific purposes allows NASWA to continue to provide access to these highly valuable services through the IDH using the Fiscal Service's Do Not Pay (DNP) Working System,

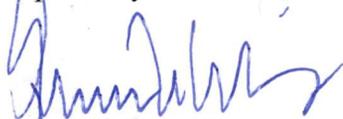
which greatly reduces its cost to utilize such services. Now that the IDH has transitioned to receiving identity verification and bank account verification capability through Fiscal Services and its vendors, only States that have signed Amendment .001 to IDH Version 6.0 agreement will be able to access those services.

As noted previously in connection with IDH Participation Agreement Versions 5.0 and 6.0, the IDH has helped identify suspicious actors who are filing UI claims in multiple States and now provides new methods for detecting fictitious employer-related fraud. By capitalizing on the affiliation with the Fiscal Service, CESER is able to obtain access to ongoing resources for Identity Verification and Bank Account verification services at a substantially reduced cost, which provides greater sustainability for the availability of these tools to the States.

Participating in the IDH greatly enhances NHES' fraud prevention capabilities at no cost to the State of New Hampshire. Other than the changes associated with using Fiscal Services' Do Not Pay system for IDV and BAV, the IDH Participation Agreement remains unchanged and is effective through September 30, 2027. Your approval of the amendment to the agreement is requested.

New Hampshire Employment Security has determined that the vendor is in good standing with the Secretary of State's Office, and has provided evidence of authority to execute and be bound by the contract. Documents supporting these assertions are available at the agency, for review upon request.

Respectfully submitted,



George N. Copadis  
Commissioner



**Unemployment Insurance Integrity Center**

***Integrity Data Hub (IDH)***

**Participation Agreement**

**Amendment (NH)-V6-001**

**PURPOSE**

The purpose of this amendment to the Integrity Data Hub Participation Agreement, Version 6.0 dated February 29, 2024, between the National Association of State Workforce Agencies' (NASWA) Center for Employment Security Education and Research (CESER), and the State of New Hampshire, hereinafter referred to as "State" is to amend existing language, and add Account Validation Services (AVS) and Entity (individual and business) Validation Services (EVS) provided through the U.S. Department of the Treasury, Bureau of Fiscal Services, Do Not Pay (DNP) Working System.

**AMENDMENTS**

There are two signature blocks in this Amendment, one for AVS and another for EVS, both signature blocks include the acceptance of the general updates. States accepting both AVS and EVS data sources are asked to sign both signature blocks.

**I. GENERAL**

a. Amend Section 5, Roles and Responsibilities – State, as follows:

- i. In the bulleted item, "Providing suspicious employer data to populate the Suspicious Employer Repository (SER) database", replace "Suspicious Employer Repository (SER)" with the new name "Fictitious Employer Repository (FER)".
- ii. Update Attachment 2 – IDH State Employer Data Elements to add Business Website as a Data Field as follows:

**ATTACHMENT 2 - IDH State Employer Data Elements**

DATA FIELD	COMMENTS
Business Website	Web address for Business

b. Amend Section 8, Terms and Conditions, Data Management, as follows:

- i. Under Data Collection and Storage, replace reference to "SER" with "FER" (see 1.a.i. above).
- ii. Under Data Sharing, adding underlined language to the existing first paragraph to support the IDH's focus on Advanced Analytics to read as follows:

*[Handwritten signature]*  
9/9/25

Initials sbs  
Date 09/09/2025

State acknowledges that State UI data, State employer data, and data State has identified as suspicious (which includes confidential information and PII), submitted to the IDH will be used by the IDH for cross-matching against data provided by other participating states, IDH's authorized contractors, Federal government agencies and their authorized agents and contractors, and third parties, and for advanced analytics for the purpose of identifying, preventing, and recovering improper payments in state and Federal UI programs. The data may be shared only pursuant to written agreements which include the confidentiality requirements for exchanging UI and employer data. Claimant Lookup requests and Employer Compare requests provided by individual states, DOL-OIG, and Federal law enforcement agencies (where appropriate) to the IDH are not shared with other states. Selected results that affect multiple states may be shared with affected states. IDH results, along with the associated ID for reference, are transmitted back to the requesting state that identifies the state where a match(s) occurred. The transmitted results do not include specific UI and employer data. States with matches can contact other participating states directly to obtain details and additional information as needed.

- iii. Remove Section 8, Terms and Conditions, Data Management, Identity Verification (No Effect on an Individual's Credit Score) paragraph, as we will no longer be using the service this applies to.

**DATA SOURCE AMENDMENTS – ACCESS TO AVS and/or EVS**

NASWA is moving from our current fee-based data vendors IDV/Experian and BAV/BNY to the U.S. Department of the Treasury Bureau of Fiscal Services DNP Working System data sources, including Account Validation and Entity Validation. Please note that the current IDV and BAV data sources will sunset as follows: AVS by July 31, 2025 and EVS by October 31, 2025. States need to sign the Amendment to opt into the new data sources before the sunset dates for continued coverage.

II. ACCOUNT VALIDATION SERVICE (AVS)

Amend Section 8, Terms and Conditions, Data Management, Data Sharing adding subsection "Account Validation Services" to describe the new data provider for bank account verifications and reference applicable utilization requirements, which are detailed in Exhibit A, Account Verification Terms of Use as follows:

**Account Validation Services (AVS)**

State acknowledges that participation in the AVS option with the IDH utilizes a third-party agency. The selected agency for AVS is the U.S. Department of the Treasury,

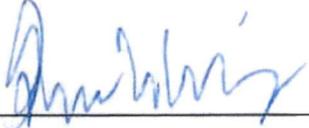
*[Handwritten signature]*  
9/9/25

Bureau of Fiscal Services, Do Not Pay Working System. To use the AVS service, States must agree to the terms in Exhibit A, Account Verification Terms of Use, Section 3.A through 3.D (see attached pgs. 6-16). For the purpose of applying Exhibit A, "Client" refers to State. By initialing and signing to select this service, State agrees to the terms in Exhibit A.

**Exhibit A is taken verbatim from CESER's Agreement with the U.S. Department of the Treasury. CESER is required to include these terms for states accessing the AVS and EVS.**

By signing below, the signatories agree to bind their respective agencies/entities to the terms and conditions of this amendment, including Section I. General and Section II. AVS. All other aspects of the original Participation Agreement between the parties remain in effect.

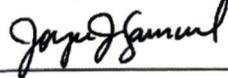
**State of New Hampshire**

By:   
Signature: \_\_\_\_\_  
Name: George N. Copedis  
Title: Commissioner  
Date: 9/9/2025

**Center for Employment Security Education and Research, Inc.**

By:   
Signature: \_\_\_\_\_  
Name: Scott B. Sanders  
Title: President and CEO  
Date: 09/09/2025

**Office of the NH Department of Justice**

By:   
Signature: \_\_\_\_\_  
Name: Joyce J. Samuel  
Title: Attorney  
Date: September 10, 2025

 Initials sbs  
Date 09/09/2025

III. ENTITY VALIDATION SERVICE (EVS)

Amend Section 8, Terms and Conditions, Data Management, Data Sharing adding subsection "Entity Validation Services" to describe the new data provider for individual and business identity verifications and reference applicable utilization requirements, which are detailed in Exhibit A, Account Verification Terms of Use as follows:

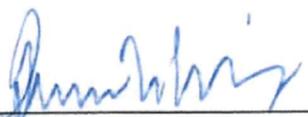
**Entity Validation Services (EVS)**

State acknowledges that participation in the EVS option with the IDH utilizes a third-party agency. The selected agency for EVS is the U.S. Department of the Treasury, Bureau of Fiscal Services, Do Not Pay Working System. To use the EVS service, States must agree to the terms outlined in Exhibit A, Account Verification Terms of Use, Section 3.A and 3.E through 3.G (see attached pgs. 6-16). For the purpose of applying Exhibit A, "Client" refers to State. By initialing and signing to select this service, State agrees to the terms in Exhibit A.

**Exhibit A is taken verbatim from CESER's Agreement with the U.S. Department of the Treasury. CESER is required to include these terms for states accessing the AVS and EVS.**

By signing below, the signatories agree to bind their respective agencies/entities to the terms and conditions of this amendment, including Section I. General and Section III. EVS. All other aspects of the original Participation Agreement between the parties remain in effect.

**State of New Hampshire**

By: \_\_\_\_\_  
Signature:   
Name: George N. Copedis  
Title: Commissioner  
Date: 9/9/25

**Center for Employment Security Education and Research, Inc.**

By: \_\_\_\_\_  
Signature:   
Name: Scott B. Sanders  
Title: President and CEO  
Date: 09/09/2025



Initials sbs  
Date -- 09/09/2025

**Amendment (NH)-V6-001 to Integrity Data Hub (IDH) Participation Agreement**

Date: 05/12/25

---

**Office of the NH Department of Justice**

By:  
Signature: Joyce J. Samuel

Name: Joyce J. Samuel

Title: Attorney

Date : September 10, 2025

*J. Samuel*  
9/9/25  
Initials sbs  
Date 09/09/2025

**EXHIBIT A**

**ACCOUNT VERIFICATION SERVICE TERMS OF USE**

**1. BACKGROUND**

U.S. Department of the Treasury, Bureau of the Fiscal Service (Fiscal Service) promotes the financial integrity and operational efficiency of the federal government through exceptional accounting, financing, collections, disbursements, and shared services. Fiscal Service, its paying agencies, and other stakeholders have been actively engaged in various initiatives to strengthen payment integrity through the mitigation and reduction of fraud and improper payments. As part of its efforts to continue to improve the integrity of financial transactions, Fiscal Service has designated a Financial Agent to implement and provide commercial account and entity validation service (collectively hereinafter referred to as "AVS" or "Services"). AVS has been designated as part of Treasury's Do Not Pay Working System and can assist Do not Pay (DNP) customers in confirming the status and ownership of a bank account. As a condition of National Association of State Workforce Agencies' (NASWA) Center for Employment Security Education and Research (CESER) Inc.'s access to and use of AVS and data provided by AVS (hereinafter, "Response Data") pursuant to the Agreement Between Fiscal Service and CESER for Do Not Pay (DNP) Services for State Unemployment Agencies (Agreement), CESER (hereinafter "Client") agrees to this Account Verification Service Terms of Use ("Terms of Use").

**2. SERVICE OVERVIEW**

**Transmission**

Fiscal Service will provide data shared by Client to Fiscal Service's Financial Agent via an AVS inquiry (hereinafter "Inquiry"). The Financial Agent and/or the Financial Agent's contractors will compare the data provided by Client to commercially available bank account and account holder data and the Financial Agent will provide the results back to Fiscal Service. Fiscal Service will, in turn, share the results with Client.

**Data Elements**

Dependent upon the level of Services (described below) Client may provide Fiscal Service with the following payment transaction related data elements: name, date of birth (DoB), address, Social Security Number (SSN), routing and transit number, and bank account number. The Financial Agent will use these data elements to validate the status and ownership of the account, validate that account information matches authoritative data sources, and/or verify a business or individual identity.

  
9/9/25

---

**Service Offerings**

- **Account Validation Services.**
  - **Account Verification:** Enables Client to submit inquiries as to whether an account number provided by Client is associated with an open account at a US financial institution. This service provides the following mapped responses:
    - Open/Valid
    - Closed/Invalid
    - Valid Pattern
    - Invalid Pattern
    - No Information Found
  - **Account Owner Authentication:** Enables Client to submit inquiries as to whether a name provided by Client matches the name of an account owner at a US financial institution associated with such account if confirmed open. This service provides the following mapped responses:
    - Ownership Match
    - Ownership No Match
    - No Information Found
  
- **Account Confidence Score Service.** Account Confidence Score Service (ACS) provides an indicator of the likelihood of fraud in connection with a beneficiary account. The Service generates a RAG rating (Red, Amber, or Green to denote low-confidence, medium-confidence, and high-confidence score ranges) and one overall Confidence Score based on the account's payment history, payment amounts, and other factors.
  
- **Entity (Identity) Validation Services.**
  - **Identity Verification:** Automates verification of personal identity data such as name, date of birth, address, phone number and government issued ID numbers, based on Client's verification criteria. This service provides the following responses:
    - "Match" or "No Match" provided for each data element provided in the input
    - Overall mapped response for the inquiry based on Client verification criteria: Pass, Needs Review, Fail, Error
    - Risk indicators\* provided when available and applicable based on inputs (e.g., deceased indicator provided when applicable)
    - Risk score\*: overall risk verification score that summarizes attribute verification, ranging from 0 (nothing found to confirm existence of individual/business) to 50 (individual/business is verified on multiple sources with no contradictory findings)  
\*May vary by data inputs
  - **Business Verification:** Automates verification of business entity data such as business name, registered principal business address, phone number and tax identification number/business registration number associated with the business, based on Client's verification criteria
    - "Match" or "No Match" provided for each data element provided in the input
    - Overall mapped response for the inquiry based on Client verification criteria: Pass, Needs Review, Fail, Error
    - Risk indicators\* provided when available and applicable based on inputs (e.g., inactive business indicator provided when applicable)

Handwritten signature and date: sbs, 9/9/25Initials sbs  
Date — 09/09/2025

- o Risk score\*: overall risk verification score that summarizes attribute verification, ranging from 0 (nothing found to confirm existence of individual/business) to 50 (individual/business is verified on multiple sources with no contradictory findings)

\*May vary by data inputs

### 3. DUTIES AND RESPONSIBILITIES OF THE CLIENT

Client acknowledges that the terms set forth in this Section 3 apply to Client's access to and use of AVS and the Response Data and Client agrees to comply with all such terms. Client acknowledges that the Financial Agent or any individual data provider (each, a "Provider") that provides Response Data through the Financial Agent may at any time cease providing one or more of the AVS service offerings. Client further acknowledges that its failure to comply with the terms herein may result in the suspension or termination of Client's access to AVS.

#### A. General Terms Related to Account Validation Services and Entity Validation Services

- i. Client agrees that it will submit Inquiries only for purposes of the Authorized Use. In addition to the Authorized Use, Client may use the Response Data, in aggregate form, for internal analytical purposes provided that the analytics relate solely to the use of the Services. Neither the foregoing language nor any other provision of this Agreement shall be interpreted to prevent Client from comparing Response Data against SWA data and other non-AVS data for the purpose of identifying, preventing, and recovering potentially improper payments for UI programs.
- ii. Client will not submit Inquiries for the purpose of searching for accounts, as opposed to verifying accounts for which payment has been proposed.
- iii. Unless otherwise permitted under the Agreement, Client shall not transmit Response data to any third party, or allow any third party to access the Response data, or sell, resell, sublicense or otherwise transfer any part of the Response data to any other person or entity, except as may be required by applicable federal, state and local laws, and the regulations promulgated thereunder.
- iv. Client acknowledges and agrees that each Response is time-sensitive and only intended to be used by Client in connection with the specific Inquiry for which it was furnished. The foregoing does not prohibit Client from utilizing the Response Data, in aggregate form, for internal analytical purposes provided that the analytics relate solely to the use of the Services.
- v. Client shall not use the Response Data to develop any service or product other than what is described in the Agreement.
- vi. None of the Response Data or Responses provided through Services constitute a "consumer report" as defined in 15 U.S.C. § 1681a(d) of the Fair Credit Reporting Act ("FCRA") (15 U.S.C. § 1681 et seq.) and none of the Services are provided to be used, and shall not be used, as a factor in determining a consumer's eligibility for any purpose covered by the FCRA. Responses, including Responses that do not provide positive Account or Entity status confirmation, may not be used as the basis to deny the provision of any goods or services. Client shall not use the Response Data (i) in whole or in part for the purpose of serving as a factor in establishing a consumer's eligibility for credit or insurance to be used primarily for personal, family, or household purposes; employment purposes; or any other authorized purpose for use of a consumer report under applicable law, or (ii) to take "adverse action" against any consumer as defined in the FCRA (15 USC § 1681a (k)(1)).

  
9/9/25

Initials sbs  
Date 09/09/2025

- vii. Client will not retain the Data or merge, aggregate, or compile Response Data into any database other than what is described in the Agreement, provided the foregoing shall not apply to prevent Client from notating account validation results associated with potential or completed transactions, aggregating or compiling Response Data for internal analytical purposes provided that the analytics relate solely to the use of the Response Data, or complying with applicable law or regulation or documented internal document retention policies.
- viii. Client agrees that if Client receives notice, from any source, that any officer, employee, contractor, agent, or authorized third-party customer of Client that has access to Response Data or has decision-making authority on how the Service is used is the subject of an investigation or other action pertaining to the use of the Response Data by any federal, state or local governmental, administrative or regulatory body, Client will immediately notify Fiscal Service of such investigation or other action, unless prohibited by law. Client further acknowledges that such investigation or action may result in termination of access to the Response Data.
- ix. To the extent this Agreement authorizes Client to disclose Response Data to certain third-party customers, Client will establish and maintain procedures for assessing its customers and shall establish safeguards to ensure that it shares Response Data only with authorized customers for authorized purposes. Client shall not permit a potential customer to access Response Data if Client has reasonable grounds to believe that a potential customer has made any material misrepresentation to Client or will misuse the Response Data for other than authorized purposes. Upon Fiscal Service's reasonable written request (not to exceed once per annum), Client shall provide Fiscal Service with information relating to its procedures for customer enrollment to enable verification of Client's compliance with this section.
- x. Except as required by law or with the Fiscal Service's prior written consent, Client will not name Financial Agent or refer to its use of the Services in any press releases, advertisements, promotional or marketing materials, or make any other third-party disclosures regarding its use of the Services.

**B. Additional Terms Applicable to Financial Agent's JPMorgan Proprietary Data Service – Account Validation Service.**

- i. Client shall not, and shall not permit any other party, to merge, aggregate or compile JPMorgan Proprietary Data Service Responses into any third party database for any purpose; provided the foregoing shall not prohibit the retention of JPMorgan Proprietary Data Service Responses for the following purposes: (i) to comply with applicable law or regulation or documented internal document retention policies, (ii) to notate the account validation results associated with potential or completed transactions in a Client record; (iii) in aggregate form, for Client's internal analytical purposes provided that the analytics relate solely to the use of the Services or (iv) copies made during routine system back-ups, in which case, such Responses may be retained for a period consistent with Client's standard procedures with respect to erasing, destroying or over-riding back-up media.
- ii. Client acknowledges that the JPMorgan Proprietary Database, including associated databases and other components of the JPMorgan Proprietary Data Service, are owned by the Financial Agent and contain valuable proprietary information of the Financial Agent. The Financial Agent retains all rights, title and interest in and to the JPMorgan Proprietary Database, including any enhancements or modifications thereto. Client agrees that it shall not attempt to reverse engineer, recreate or otherwise copy the JPMorgan Proprietary Database or JPMorgan Proprietary Data Service and shall not assist any other person, directly or indirectly, in any attempt to reverse engineer, recreate or otherwise copy the JPMorgan Proprietary Database or JPMorgan Proprietary

*[Handwritten signature]*  
9/19/25

Initials sbs  
Date 09/09/2025

Database Service.

**C. Terms Applicable to Financial Agent's JPMorgan Proprietary Data Service – Account Confidence Score.**

- i. A low Confidence Score will not prevent Client from initiating a payment or other transaction to the subject account. Client will not rely on the Confidence Score with no human review. Client agrees that it will take into account all relevant factors (including the Confidence Score) when making a decision about whether to make a payment to the account. Should a transaction thereafter be initiated to an account with the Financial Agent, all standard processing, screening and reviews will be performed by Financial Agent; such screening/reviews may or may not cause such transaction to alert or be rejected. Client is fully responsible for any decisions Client makes based on a Confidence Score or associated RAG indicators received under the Service, and for any payments or transactions initiated to the subject account and Financial Agent will have no responsibility or liability for any losses incurred by Client as a result of such decisions.
- ii. Client agrees that it will not use the Confidence Score as the sole determinant of whether or not to initiate or complete a payment; any reliance Client places on the Confidence Score is strictly at Client's risk. Should Client receive a low Confidence Score or No Information Found Response for a prospective payment, it will not decline to complete a transaction without taking additional intermediate steps such as requesting alternate account information. Client understands that a Confidence Score is an indicator that Financial Agent has seen transactions to the subject account clear successfully previously and is not an assurance that the prospective transaction will be successfully completed.
- iii. Client acknowledges that its use of the results from the Confidence Score Service is subject to Section A, above, and this Section C.
- iv. Except as required by law or with Fiscal Service's prior written consent, Client will not name Financial Agent or refer to its use of the Services in any press releases, advertisements, promotional or marketing materials, or make any other third-party disclosures regarding its use of the Services.

**D. Additional Terms Applicable to the Verify Account Service – an Account Validation Service**

- i. The Verify Account Service will provide Response Data only to be used to verify that the recipient or the initiator of a payment, as the case may be, is the owner of, or authorized to transact on, the bank account which the payment is being deposited into or is being drawn from, as the case may be, and to confirm whether that bank account is open or closed.
- ii. Client shall not knowingly permit any of its directors, officers, employees, contractors, subcontractors, attorneys, auditors and accountants, to access the Service, if the person has been convicted of a crime in connection with: (a) a dishonest act, breach of trust, or money laundering, or has agreed to enter into a pretrial diversion or similar program in connection with a prosecution for such offense, as described in Section 19 of the Federal Deposit Insurance Act, 12 U.S.C. § 1829(a); or (b) a felony.
- iii. Client shall not merge, aggregate, or compile Response Data into any other database for use in connection with future Inquiries; provided that the foregoing limitation shall not prevent Client from notating account validation results associated with potential or completed transactions or prevent Client from aggregating or compiling Response Data for internal analytical purposes provided that the analytics relate solely to the use of the Services.



- iv. Client shall promptly notify Fiscal Service of any complaint or dispute by or between Client and any person or entity directly relating to (a) Inquiries for the Verify Account Service, or (b) Verify Account Service Response Data.

**E. Additional Terms Applicable to Customer ID, gIdentify Consumer Standard and gIdentify Business Standard – Entity Validation Services.**

- i. The Customer ID, gIdentify Consumer Standard and gIdentify Business Standard Services will be used by Client solely to perform Transactions for purposes of the Authorized Use. Client may not use these Services for the benefit of any third party other than a third party expressly authorized pursuant to the Agreement. For purposes of this section, "Transaction(s)" means any verification or other transaction, completed or submitted by Client.
- ii. Client certifies that because the information provided under these Services is not consumer report information under FCRA, Client will not request or use these Services as a factor in establishing a consumer's eligibility for credit or insurance to be used primarily for personal, family, or household purposes, employment purposes, tenant screening, or for any other purpose authorized under the FCRA or similar state or local statute, rules or regulation.
- iii. Client understands and agrees that it is solely responsible for any decisions it makes or actions it takes in connection with information provided by these Services.
- iv. Client will establish and maintain such security and privacy measures and procedures as are required by applicable law and that which are reasonably practicable to provide for the safe custody, control and access of any (i) Data, and (ii) to prevent unauthorized access thereto or use thereof. Client agrees that Client (or Client's authorized end user customer, as applicable) is solely responsible for verifying the accuracy and completeness of all submitted Transactions.
- v. Client affirms and agrees that it will not transfer, process, store, or access these Services or Responses provided by Financial Agent in connection with these Services outside of the United States without Fiscal Service's written consent.
- vi. Client agrees it will not use the Services for any marketing purposes, including but not limited to creating a telemarketing call list or direct mailing list.

**F. Additional Terms Applicable to Consumer InstantID and Business InstantID - Entity Validation Services.**

- i. Client acknowledges that the Consumer InstantID and Business InstantID products and services and related information provided by the Provider through the Financial Agent hereunder (collectively, the "CIID and BIID Data" or "Services") are and shall remain the property of Provider and Client shall do nothing inconsistent with the copyright or other proprietary rights of Provider in and to the CIID and BIID Data.
- ii. Client is authorized to use the Services solely for the Authorized Use. Client represents and warrants that it will not use the Services for any other purpose including in violation of any applicable laws nor for the purpose of creating its own repository related to, including but not limited to, driving record history. Client further represents and warrants that (i) to the extent the Services accessed by Client include non-public personal information protected by the Gramm-Leach-Bliley Act (GLBA), the following GLBA permissible use applies: Fraud Prevention or Detection (For use to protect against or prevent actual or potential fraud, unauthorized or improper transactions, claims, or other liability), and (ii) to the extent the Services accessed by Client include specific information protected by the Driver's Privacy Protection Act, (18 U.S.C. § 2721 et

*[Handwritten signature]*  
9/9/25

seq.) and related state laws, the following DPPA permissible use applies: Government Agency (For use by any government agency in carrying out its functions).

- iii. Client shall not use the CIID and BIID Data as the sole determinant of whether or not to initiate or complete a proposed payment.
- iv. Client may not use the CIID and BIID Data to create a competing product. Client agrees that it shall not reproduce, retransmit, republish, or otherwise transfer the Services for any commercial purposes. Client shall comply with all laws, regulations and rules which govern the use of the CIID and BIID Data and information provided therein. Client agrees that it will not transfer, process, store, or access the Services outside of the United States without Financial Agent's written consent.
- v. Non-FCRA Use Restrictions. The Services (described hereinafter as the "Non-FCRA Services") are not provided by "consumer reporting agencies," as that term is defined in the Fair Credit Reporting Act (15 U.S.C. § 1681, et seq.) ("FCRA") and do not constitute "consumer reports," as that term is defined in the FCRA. None of the Non-FCRA Services are provided to be used, and shall not be used, as a factor in determining a consumer's eligibility for any purpose covered by the FCRA. Responses, including Responses that do not provide positive Account or Entity status confirmation, may not be used as the basis to deny the provision of any goods or services. Client shall not use the Response Data (i) in whole or in part for the purpose of serving as a factor in establishing a consumer's eligibility for credit or insurance to be used primarily for personal, family, or household purposes; employment purposes; or any other authorized purpose for use of a consumer report under applicable law, or (ii) to take "adverse action" against any consumer as defined in the FCRA (15 USC § 1681a (k)(1)). For clarity, the Non-FCRA Reseller Services may not be used in whole or in part as a factor in determining eligibility for a license or other benefit granted by a government agency required by law to consider an applicant's financial responsibility or status. Client will not use the Non-FCRA Services in connection with collection of a consumer debt.
- vi. DPPA Data. Some of the information contained in the Services is "personal information," as defined in the Driver's Privacy Protection Act, (18 U.S.C. § 2721 et seq.) and related state laws (collectively, the "DPPA"), and is regulated by the DPPA ("DPPA Data"). Client shall not obtain and/or use DPPA Data through the Services in any manner that would violate the DPPA. Client acknowledges and agrees that it may be required to certify its permissible use of DPPA Data at the time it requests information in connection with certain Services and will recertify upon request by Fiscal Service or the Financial Agent.
- vii. Additional Terms. To the extent applicable, insofar as the Services accessed by Client include information or data described in the Risk Supplemental Terms contained at: [www.lexisnexis.com/terms/risksupp](http://www.lexisnexis.com/terms/risksupp), Client agrees to comply with the Risk Supplemental Terms set forth therein, unless otherwise prohibited by law. The Risk Supplemental Terms are hereby incorporated into this Agreement by reference. In the event of a direct conflict between this Agreement and the Risk Supplemental Terms, the order of precedence shall be as follows: this Agreement and then the Risk Supplemental Terms. Notwithstanding the foregoing, Fiscal Service acknowledges that the Response Data provided to Client does not reveal the underlying data described in the Risk Supplemental Terms.
- viii. MVR Data. If Client is permitted to access Motor Vehicle Records ("MVR Data"), without in any way limiting Client's obligations to comply with all state and federal laws governing use of MVR Data, the following specific restrictions apply and are subject to change:

  
9/9/25

Initials sbs  
Date 09/09/2025

- Client shall not use any MVR Data, or portions of information contained therein, to create or update a file that Client uses to develop its own source of driving history information.
  - As requested by Fiscal Service, Client shall complete any state forms that Financial Agent is legally or contractually bound to obtain from Client before providing Client with MVR Data.
  - Fiscal Service may conduct reasonable and periodic reviews of Client use of MVR Data. In response to any such review, Client must be able to substantiate the reason for each MVR Data order.
- ix. HIPAA. Client represents and warrants that Client will not provide Fiscal Service and/or Financial Agent with any Protected Health Information (as that term is defined in 45 C.F.R. Sec. 160.103) or with Electronic Health Records or Patient Health Records (as those terms are defined in 42 U.S.C. Sec. 17921(5), and 42 U.S.C. Sec. 17921(11), respectively) or with information from such records.
- x. Economic Sanctions Laws. Client acknowledges that Financial Agent is subject to economic sanctions laws, including but not limited to those enforced by the U.S. Department of the Treasury's Office of Foreign Assets Control ("OFAC"), the European Union, and the United Kingdom. Accordingly, Client shall comply with all economic sanctions laws of the United States, the European Union, and the United Kingdom. Client shall not provide access to the Services to any individuals identified on OFAC's list of Specially Designated Nationals ("SDN List"), the UK's HM Treasury's Consolidated List of Sanctions Targets, or the EU's Consolidated List of Persons, Groups, and Entities Subject to EU Financial Sanctions. Client shall not take any action which would place Financial Agent in a position of non-compliance with any such economic sanctions laws.
- xi. Retention of Access Records. For uses of GLBA Data, DPPA Data and MVR Data, Client (or Client's authorized end user customer, as applicable) shall maintain for a period of five (5) years a complete and accurate record (including consumer identity, purpose and, if applicable, consumer authorization) pertaining to every access to such data.
- xii. If the Services involve the access to or handling of CIID and BIID data, Client shall promptly notify Fiscal Service in the event that Client is unable to comply with the data security, data retention and data destruction obligations in this Section F.
- xiii. SECURITY. Client shall (i) keep all user identification numbers, and related passwords, or other security measures (collectively, "User IDs") confidential and prohibit the sharing of User IDs; (ii) immediately deactivate the User ID of any employee or contractor who no longer has a need to know, or for terminated employees on or prior to the date of termination; (iii) maintain and enforce data destruction procedures to protect the security and confidentiality of all information obtained through the Services as it is being disposed; (iv) be capable of receiving the Services where the same are provided utilizing "secure socket layer," or such other means of secure transmission as is deemed reasonable by Financial Agent; (v) not access and/or use the Services via mechanical, programmatic, robotic, scripted or other automated search means, other than through batch or machine-to-machine applications approved by Financial Agent; (vi) take all steps to protect their networks and computer environments, or those used to access the Services, from compromise; (vii) as applicable, periodically review searches to ensure that searches were performed for a legitimate business purpose and in compliance with all terms and conditions herein; and (viii) maintain policies and procedures to prevent unauthorized use of User IDs and the Services. Client will immediately notify Fiscal Service, if Client suspects, has reason to believe or confirms that a



User ID or the Services (or data derived directly or indirectly therefrom) is or has been lost, stolen, compromised, misused or used, accessed or acquired in an unauthorized manner or by any unauthorized person, or for any purpose contrary to the terms and conditions herein. Furthermore, in the event that the Services provided to Client include personally identifiable information (including, but not limited to, social security numbers, driver's license numbers or dates of birth), the following shall apply: Client acknowledges that, upon unauthorized acquisition or access of or to such personally identifiable information, including but not limited to that which is due to use by an unauthorized person or due to unauthorized use (a "Security Event"), Client shall, in compliance with law, notify the individuals whose information was potentially accessed or acquired that a Security Event has occurred, and shall also notify any other parties (including but not limited to regulatory entities and credit reporting agencies) as may be required in Financial Agent's reasonable discretion. Client agrees that such notification shall not reference Financial Agent or the product through which the data was provided, nor shall Financial Agent be otherwise identified or referenced in connection with the Security Event, without Financial Agent's express written consent. Client shall provide samples of all proposed materials to notify consumers and any third-parties, including regulatory entities, to Fiscal Service for review and approval prior to distribution. In the event of a Security Event, Fiscal Service may, in its sole discretion, take immediate action, including suspension or termination of the Services to Client, without further obligation or liability of any kind.

- xiv. CONFIDENTIALITY. Client ("Receiving Party") acknowledges that it may have access to confidential information of the Provider ("Disclosing Party"), such as CIID or BIID Data, (whether written or oral) ("Confidential Information"). Confidential Information shall not include information that: (i) is or becomes (through no improper action or inaction by the Receiving Party) generally known to the public; (ii) was in the Receiving Party's possession or known by it prior to receipt from the Disclosing Party; (iii) was lawfully disclosed to Receiving Party by a third-party and received in good faith and without any duty of confidentiality by the Receiving Party or the third-party; or (iv) was independently developed without use of any Confidential Information of the Disclosing Party by employees of the Receiving Party who have had no access to such Confidential Information. The Receiving Party agrees not to divulge any Confidential Information or information derived therefrom to any third-party, except those specifically authorized in the Agreement, and shall protect the confidentiality of the Confidential Information with the same degree of care it uses to protect the confidentiality of its own confidential information, but in no event less than a reasonable degree of care. Notwithstanding the foregoing, the Receiving Party may disclose Confidential Information to the extent required by subpoena, court order or other governmental authority, provided that the Receiving Party shall give the Disclosing Party prompt written notice of such subpoena, court order or other governmental authority so as to allow the Disclosing Party to have an opportunity to obtain a protective order to prohibit or restrict such disclosure at its sole cost and expense. Confidential Information disclosed pursuant to subpoena, court order or other governmental authority shall otherwise remain subject to the terms applicable to Confidential Information. The Receiving Party's obligations with respect to Confidential Information shall continue for the term of the Agreement and for a period of five (5) years thereafter. Notwithstanding the foregoing, if Receiving Party is bound by the Freedom of Information Act, 5 U.S.C. 552, or other federal, state, or municipal open records laws or regulations which may require disclosure of information, and disclosure thereunder is requested, Receiving Party agrees that it shall notify Financial Agent in writing and provide Financial Agent an opportunity to object, if so permitted thereunder, prior to any disclosure.
- xv. Other than as provided herein, Client will not duplicate or compile or re-use any data contained in the CIID and BIID Data and shall not retain it for any purpose, and further shall purge the CIID



Initials sbs  
Date 09/09/2025

and BIID Data within 90 days of receipt. Notwithstanding the foregoing, Client may retain administrative CIID and BIID Data (i) to administratively notate the validation results associated with potential or completed transactions; (ii) in aggregate form, for internal analytical purposes provided that the analytics relate solely to the use of the Services; or (iii) for purposes of complying with applicable law or regulation or documented internal document retention policies.

- xvi. Client shall not conduct any analyses of the CIID and BIID Data nor shall Client use, or allow to be used, any information it obtains as a result of its handling, processing or possession of the CIID and BIID Data in connection with the creation, promotion, marketing, selling and/or licensing of Client's own information, products or services. Client acknowledges that the CIID and BIID Data is time sensitive and shall only be used in connection with the specific inquiry for which it was requested. After the immediate inquiry, CIID and BIID Data is no longer live data and instead viewed as administrative data. Neither the foregoing restriction nor anything else in this Agreement shall prohibit Client from notating administration validation results or utilizing the administrative notations, in aggregate form, for internal analytical purposes, provided that the analytics relate solely to the use of the Services. For clarity, as part of the use or testing of the Entity Validation Services, Client shall not create any derivative work using the Entity Validation Services that are comprised of Provider risk codes, Provider scoring, and Provider filing date.
- xvii. Client shall (a) use the CIID and BIID Data solely in connection with payments anticipated to be made to or received from the person or entity that is associated with the CIID and BIID Data, and (b) not to further disclose or distribute the CIID and BIID Data to any third party, except as otherwise provided in this Agreement.
- xviii. Fiscal Service will have the right to review Client's use of the CIID and BIID Data to assure compliance with the terms of this Section F and any other legal or regulatory requirements. Client shall fully cooperate with Fiscal Service in connection with such reviews and will provide Fiscal Service access to such Client records and personnel as Fiscal Service may reasonably require for such purpose subject to Client's security requirements.
- xix. Client agrees to destroy, in accordance with industry best practices and any applicable legal or regulatory requirements, the CIID and BIID Data and any copies or derivative thereof immediately upon termination of the Service, and upon request, to certify such destruction to Fiscal Service. Notwithstanding the foregoing, Client may retain administrative CIID and BIID Data (i) to administratively notate the validation results associated with potential or completed transactions; (ii) in aggregate form, for internal analytical purposes provided that the analytics relate solely to the use of the Services; or (iii) for purposes of complying with applicable law or regulation or documented internal document retention policies.
- xx. Client acknowledges that in addition to this Section F, the terms and conditions set forth in Sections 3.A and 3.E also apply to Client's access and use of the CIID and BIID Data.

**G. Additional Terms Related to Other Entity Validation Services.**

- i. Client acknowledges that Response Data is current as of the time it is provided and the Financial Agent has no obligation to update any Response Data after it has been provided or to notify Client if such Response Data has changed.
- ii. Client acknowledges and agrees that each Response is time-sensitive and only intended to be used by Client in connection with the specific Inquiry for which it was furnished. Accordingly, Client

Handwritten signature and date in blue ink.

---

acknowledges and agrees that it will not use the Response Data in connection with any subsequent Inquiry.

- iii. The Response Data is and shall remain the property of the respective Provider and/or the Financial Agent. Client shall do nothing inconsistent with the copyright or other proprietary rights of the Provider and/or the Financial Agent in and to the Response Data.
- iv. Client represents and warrants that, to the extent the Gramm- Leach-Bliley Act (15 USC § 6801 et seq.) (GLBA) is applicable, it will use the information obtained from the Entity Validation Service only for purpose(s) consistent with the GLBA, including the GLBA's limits regarding reuse of information found at 15 USC § 6802(c) and exceptions thereto found at 15 USC § 6802(e).

09/09/2025

*[Handwritten Signature]*  
9/9/25

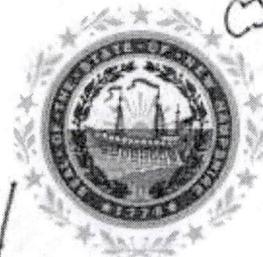


"We're working to keep New Hampshire working"

GEORGE N. COPADIS, COMMISSIONER

RICHARD J. LAVERS, DEPUTY COMMISSIONER

LEGAL SECTION  
45 SOUTH FRUIT STREET  
CONCORD, NH 03301-4857



44

October 1, 2024

His Excellency, Governor Christopher T. Sununu  
and the Honorable Council  
State House  
Concord, NH 03301

**REQUESTED ACTION**

To authorize New Hampshire Employment Security (NHES) to enter into a **sole source** Integrity Data Hub (IDH) Participation Agreement Version 6.0 with the National Association for State Workforce Agencies' (NASWA's) Center for Employment Security Education and Research, Inc. (CESER), located at 444 N. Capitol Street, NW Suite 300, Washington, DC, from the date of Governor and Council approval through September 30, 2027.

**EXPLANATION**

During the pandemic, a serious problem arose with fraudulent Unemployment Insurance (UI) claims being filed across the country. This occurred in large part through the filing of claims by criminal enterprises using stolen identities. Even before the pandemic, there was significant concern regarding the potential for fraud in the payment of UI benefits. For this reason, the National Association of State Workforce Agencies (NASWA) worked with the United States Department of Labor (USDOL) to develop an Integrity Data Center and Integrity Data Hub (IDH), to facilitate cross-matching of suspicious UI claims information by and between the States. CESER has a Cooperative Agreement with USDOL to operate the Integrity Data Center and IDH. States must enter into a "Participation Agreement" to engage in the resulting data exchange network. NHES is authorized by law to participate in the IDH and received Governor & Council approval to enter into IDH Participation Agreement Version 5.0 in September of 2021.

Participation by the States in the IDH includes the submission of suspicious actor data and UI claims data, and States receiving associated lookup/matching/analysis results from the IDH and associated applications as defined in the Agreement. Since the last Participation Agreement was signed, the IDH has been expanded to include provisions for the collection of employer data, to include information on fraudulent employers as well as new employer registrations. This update was undertaken to support the Center's development of a new Employer Data Module (EDM) as part of the IDH. The initial version of the EDM will collect information on fraudulent employers identified by States in a Fictitious Employer Repository (FER) and cross-match new employer registrations against the FER to identify potential fraud. The EDM will be expanded incrementally to include additional functionality

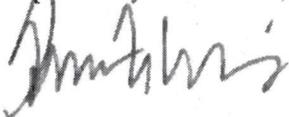
such as validation checks on new employer registrations, additional cross-matching of employer data against other IDH data (UI claimants), and verification of employer bank accounts. The EDM provides much needed capability to States to combat emergent employer-related fraud affecting the Unemployment Insurance community.

The Agreement has also been expanded to include provisions for NASWA/CESER to be designated as an agent of the State in specific transactions with the US Treasury Bureau of Fiscal Service (Fiscal Service). NASWA is working closely with Fiscal Service to obtain access to new data sources and to provide alternative capabilities that currently exist within IDH, specifically Identity Verification (IDV) and Bank Account Verification (BAV) solutions, through Fiscal Service. NASWA/CESER's designation as an agent of the state for these specific purposes will allow NASWA to continue to provide access to these highly valuable services through the IDH. Once the IDH has transitioned to receiving ID verification and bank account verification capability through Fiscal Services, only states that have signed this revised agreement will be able to access those services.

There is no cost to the State for participating in the IDH. Over the course of many Unemployment Insurance Program Letters (UIPLs), USDOL first recommended and then admonished States to take advantage of the fraud prevention benefits provided through participation in the IDH. In particular, the IDH has helped identify suspicious actors who are filing UI claims in multiple States, and now provides new methods for detecting fictitious employer-related fraud.

IDH continues to provide the opportunity for New Hampshire to work smarter by streamlining and better deploying limited resources in coordination with other States in order to effectively fight back against a national problem and continue to protect our Unemployment Compensation Trust Fund. Participating in the IDH will greatly enhance NHES' fraud prevention capabilities and reduce the amount of manual work that is currently being done to identify fraudulent claims before payments are made.

Respectfully submitted,



George N. Copadis  
Commissioner



GEORGE N. COPADIS, COMMISSIONER

RICHARD J. LAVERS, DEPUTY COMMISSIONER

September 16, 2021  
SEP 17 '21 AM 8:53 RCVD

His Excellency, Governor Christopher T. Sununu  
and the Honorable Council  
State House  
Concord, NH 03301

**REQUESTED ACTION**

To authorize New Hampshire Employment Security (NHES) to enter into a sole source Integrity Data Hub (IDH) Participation Agreement with the National Association for State Workforce Agencies' (NASWA's) Center for Employment Security Education and Research, Inc. (CESER)(hereinafter CESER), 444 N. Capitol Street, NW Suite 300, Washington, DC, from the date of Governor and Council approval through September 30, 2026.

**EXPLANATION**

Throughout the COVID-19 pandemic, there has been a very serious problem with fraudulent Unemployment Insurance (UI) claims being filed across the country resulting from identities stolen from large scale breaches occurring outside of the unemployment system. Even before the pandemic, there was a high level of concern about the potential for fraud in the payment of UI benefits. For this reason, the National Association of State Workforce Agencies (NASWA) had been working with the United States Department of Labor (USDOL) to develop an Integrity Data Center and "Integrity Data Hub" (IDH), to facilitate cross-matching of UI claims information by and between the States. CESER currently has a Cooperative Agreement with USDOL to operate the Integrity Data Center and IDH. States must enter into a "Participation Agreement" to be a part of the resulting data exchange network. As part of the recent state budget, NHES was authorized to participate in IDH as long as appropriate data safeguards were in place.

As noted in the Participation Agreement, "[t]he purpose of the IDH is to provide State[s] with a Center managed data hub where UI Claims data can be analyzed and cross matched with UI data from other states and various fraud detection sources designed to assist in the detection and prevention of fraudulent activity." Participation by the States in the IDH includes States submitting "suspicious actor data and UI claims data, and State[s] receiving associated lookup/matching/analysis results from the IDH and associated applications" as defined in the Agreement.

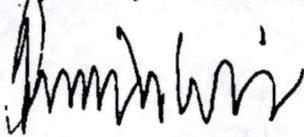
There is no cost to the States for participating in the IDH. Over the course of many Unemployment Insurance Program Letters (UIPLs), USDOL first recommended and then admonished States to take advantage of the fraud prevention benefits provided through

His Excellency, Governor Christopher T. Sununu  
and the Honorable Council  
Page 2 of 2

participation in the IDH. In particular, the IDH helps identify suspicious actors who are filing UI claims in multiple States.

New Hampshire has done an incredible job throughout the pandemic at detecting fraudulent claims prior to payment. However, this work has largely fallen on the backs of the dedicated men and women of the Department. This type of dependency is not sustainable. IDH provides the opportunity for New Hampshire to work smarter by streamlining and better deploying limited resources in coordination with other States in order to effectively fight back against a national problem and continue to protect our employer paid Unemployment Compensation Trust Fund. Participating in the IDH will greatly enhance NHES' fraud prevention capabilities and reduce the amount of manual work that is currently being done to identify fraudulent claims before payments are made.

Respectfully submitted,

A handwritten signature in black ink, appearing to read "George N. Copadis". The signature is fluid and cursive, with a prominent initial "G" and "C".

George N. Copadis  
Commissioner