



**Unemployment Insurance Integrity Center**

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

**Participation Agreement**

Version: 5.0

G072DOLT22

## Table of Contents

1.	Agreement.....	3
2.	Introduction.....	3
3.	Background.....	3
4.	Roles and Responsibilities – CESER.....	3
5.	Roles and Responsibilities - State.....	4
6.	Period of Performance .....	4
7.	Project Contacts .....	4
8.	Terms and Conditions.....	5

## 1. AGREEMENT

This Agreement is by and between the National Association of State Workforce Agencies' (NASWA) Center for Employment Security Education and Research, Inc. (CESER) and the U.S Virgin Islands Department of Labor, hereinafter referred to as "State".

## 2. INTRODUCTION

This document defines an Agreement between CESER and State for participation in the Integrity Data Hub (IDH). Participation includes State submitting suspicious actor data and UI claims data, and State receiving associated lookup/matching/analysis results from the IDH and associated applications as defined in this agreement.

## 3. BACKGROUND

About the Unemployment Insurance (UI) Integrity Center

Overpayments, errors, and instances of fraud within the UI program have been long-standing concerns for Congress, the Federal Office of Management and Budget (OMB), the U.S. Department of Labor (USDOL), and SWAs. To address these concerns, the USDOL and SWAs have initiated strategies and initiatives designed to reduce the risk of overpayments and prevent fraud.

NASWA's subsidiary, CESER, is the lead organization responsible for operation of the UI Integrity Center (Center). The Center is charged with developing "innovative UI program integrity strategies to reduce improper payments, prevent and detect fraud, and recover any improper payments made" (UIPL 28-12).

Purpose of the IDH

The purpose of the IDH is to provide States, OIG, and federal law enforcement agencies that meet the definition of a "public official" as defined by 20 C.F.R. 603.2(d) 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 in UI programs.

## 4. ROLES AND RESPONSIBILITIES – CESER

CESER shall be responsible for coordinating with State and managing the IDH. Specific responsibilities shall include:

- Project management, including preparation and maintenance of the IDH development and enhancement project plan/schedule;
- Scheduling/coordinating meetings, working sessions and reviews as needed;
- Documenting system functional and operational business requirements, including security requirements;
- Developing the system technical architecture/design;
- Developing and maintaining the IDH including all associated system documentation;
- Implementing and maintaining a secure, FedRAMP compliant IT infrastructure and ensuring all required updates and security systems are in place;

- Planning, coordinating, and assisting in system testing;
- Coordinating system implementation with States, DOL-OIG, and with federal law enforcement agencies, when appropriate;
- Developing measures to evaluate performance/value;
- Preparing data sharing agreements as needed;
- Providing resources, as available, to States to support participation in the IDH project;
- Establishing agreements and Non-Disclosure Agreements (NDA's) with all CESER authorized contractors; and
- Ensuring all transmissions are secure using the appropriate NIST/security standards.

## 5. ROLES AND RESPONSIBILITIES - STATE

State shall provide UI program and technical/IT personnel to assist with IDH implementation efforts. Specific responsibilities shall include:

- Providing suspicious actor data to populate the Suspicious Actor Repository (SAR) database (specific data elements to be provided are listed in Attachment 1);
- Providing initial and continued claims for matching and analysis (specific data elements to be provided are listed in Attachment 1);
- Receiving results from the IDH for analysis and appropriate action;
- Providing input on IDH usage and potential impact on workflows and business rules;
- Designating an IDH State Administrator to manage State user types and roles; and
- Participating in system testing, implementation, and evaluation.

## 6. PERIOD OF PERFORMANCE

This Agreement shall be valid for a five (5) year period beginning on date the agreement is executed and may be extended upon mutual agreement of both parties. The Agreement may be terminated by either party, in accordance with the Termination of Agreement clause in this Agreement.

## 7. PROJECT CONTACTS

Table 1 defines the primary project leadership points of contact for the IDH.

**Table 1: IDH Project Contacts**

Name	Title	Telephone	Email
Jerome Lord	Sr. Program Analyst	(406)422-9379	<a href="mailto:jlord@naswa.org">jlord@naswa.org</a>
Mark Richmond	Program Analyst	(208)860-8949	<a href="mailto:mrichmond@naswa.org">mrichmond@naswa.org</a>
Kendrah Gonzalez	Program Analyst	(531)739-9443	<a href="mailto:kgonzalez@naswa.org">kgonzalez@naswa.org</a>
James Cotter	Project Director	(703)587-8353	<a href="mailto:jcotter@naswa.org">jcotter@naswa.org</a>

Table 2 defines the primary project leadership points of contact for State. This list should include State Business lead, State Technical lead, and others as deemed appropriate.

**Table 2: USVI IDH Project Contacts**

<b>Name</b>	<b>Title</b>	<b>Telephone</b>	<b>Email</b>
Beryl Todman	Integrity Program Coordinator	(340)776-3700	beryl.todman@dol.vi.gov
Roger Richards	Director - IT	(340) 773-1994	roger.richards@dol.vi.gov
Trevor Antoine	Integrity Unit	(340) 776-3700	trevor.antoine@dol.vi.gov

**8. TERMS AND CONDITIONS**

**Voluntary Participation:** The parties have entered into this Agreement voluntarily and agree to participate in the operation and utilization of the IDH.

**Data Ownership:** All data provided by State shall remain the property of State.

**Termination of Agreement:** Either party may terminate this Agreement for any reason upon thirty (30) days written notice to the other party. In case of termination, parties will work collectively to determine disposition of collected data.

**Data Management**

Data Collection and Storage

The data elements submitted from State for analysis, cross matching, and population of the Suspicious Actor Repository, are identified on Attachment 1 – IDH Data Elements, attached to this document. Any modifications to Attachment 1 will be made only by mutual agreement of both parties.

Data submitted to the IDH by State shall be retained by CESER, for purposes of analysis and cross matching to assist in the prevention and detection of improper payments and fraud.

Data Sharing

State acknowledges that information provided on suspicious actors (SAR data) and all UI claims data submitted to the IDH will be used by the IDH and its authorized contractors for analysis and cross matching against proprietary and publicly sourced data and data provided by other participating states. Lookup requests (claim data) provided by individual states, DOL-OIG, and federal law enforcement agencies (where appropriate) to the IDH are not shared with other states. IDH results are transmitted back to the requesting state that identify the state where a match(s) occurred and the associated claim ID for reference, but do not include specific claim data. States with matches can then contact other participating states directly to obtain details and additional information as needed.

Notwithstanding the restrictions on disclosure of IDH data set out elsewhere in this agreement, CESER is authorized to report any allegations as described in item 1 below to USDOL, and to transfer the data described in both items 1 and 2 from the IDH to DOL-OIG and other federal law enforcement agencies that meet the definition of a “public official” as defined by 20 C.F.R. 603.2(d):



1. Any IDH data regarding allegations that are reasonably believed to constitute fraud, waste, abuse, mismanagement, or misconduct related to UI programs; and
2. Any cross-match hits and data directly related to cross match hits.

## Identity Verification (No Effect on Claimant Credit Score)

State acknowledges that participation in the IDH Identity Verification (IDV) option requires the use of a third-party Identity Verification vendor who is subject to provisions of Section 609 of the Fair Credit Reporting Act (FCRA). This act specifically requires an FCRA subject vendor to log the Inquiry for compliance by updating their existing vendor Transaction Log File (TLF) that such an inquiry from CESER was initiated. This Inquiry **has no impact on claimant credit score**, is not a disputable query, and is not a part of the vendor operational, search, or analysis data. The TLF entry is stored offline with access limited to CESER and regulatory auditors. In addition, CESER requires the IDV vendor to verifiably delete the PII and other data elements from their operational and searchable database. Provisions outlined in this paragraph shall be applicable to the current IDV vendor and shall remain in effect in the event of a change in IDV vendor.

## CESER Subcontractor Data Retention

State acknowledges CESER may issue subcontracts with third-party vendors to provide new IDH services and/or functionalities in the future. These subcontractors may be required to retain data for compliance with regulatory and/or audit requirements. CESER will validate requirements for subcontractor data retention and will notify State of the details of the subcontracting arrangement, including the purpose of the subcontracting, the functions the subcontractor will perform, the identity of the subcontractor, the process by which CESER selected the subcontractor, and any associated data retention requirements prior to implementation of new services and/or functionalities. State will have the ability to opt out of any IDH third-party services as they deem appropriate.

## Data Security and Confidentiality

Each participating State is subject to Federal and state laws which, with few exceptions, restrict the disclosure of such information and data by State or any agent of such State. State and CESER agree:

1. The information provided by and to the IDH shall be used solely for administration of state and federal unemployment compensation laws.
2. Access to or disclosure of IDH data shall be limited to authorized employees of State, CESER, or authorized persons who perform services for State or CESER, as set out in 20 CFR 603.9.
3. CESER will store and protect confidential UC information as set out in 20 CFR 603.9(b).
4. All data submitted to and retained by CESER will be done so using the security and encryption protocols discussed in this document and other CESER data security documents.
5. CESER shall notify the states, separate from this agreement, which contractors will be receiving the data, why CESER is working with the contractor, and what the contractor will be doing with the data.
6. The State may conduct on-site inspections to assure the requirements of the State's law and the agreement are being met.

**Provisions for a Data Breach**

A data breach shall be defined as an incident in which sensitive, protected or confidential data has potentially been viewed, stolen or used by an individual unauthorized to do so. In the event of a data breach or unauthorized disclosure of IDH data residing on State system, State will notify CESER immediately using the following contact list.

Priority Listing	Name	Title	Phone	Email
Primary	Jerome Lord	Program Analyst	(406)422-9379	<a href="mailto:jlord@naswa.org">jlord@naswa.org</a>
Secondary	James Cotter	Project Manager	(703)587-8353	<a href="mailto:jcotter@naswa.org">jcotter@naswa.org</a>
Alternate 1	Rich Thielman	IT Security Mgr.	(202)329-4227	<a href="mailto:rthielman@naswa.org">rthielman@naswa.org</a>

State shall continue to notify CESER representatives until State receives confirmation that their message regarding a potential breach has been received by CESER. CESER will suspend State access to the IDH until both parties agree the data is reasonably secured from further data breaches or unauthorized disclosure.

In the event of a data breach or unauthorized disclosure at CESER, CESER will notify State, and will address the breach in accordance with the latest version of the *Center Data Breach Policy*.

**IDH Access/Use:**

- CESER IDH Administrator shall be designated by the CESER Project Director.
- State IDH Administrator shall be approved by State UI Director, or his/her designee.
- State users of the IDH shall be approved by State IDH Administrator.
- All IDH user access and permissions shall be verified, at a minimum, twice each year. Validation shall be performed by the state IDH Administrator through workflows within the IDH.
- All IDH users shall not allow the sharing of IDH user login and password information.

IDH is intended to flag suspicious claims and/or potentially suspicious activity. As such, State shall not establish an improper payment on a claim based solely on IDH data. Independent verification of the data and appropriate investigation must be conducted by State in accordance with Unemployment Insurance Program Letter (UIPL) No.1-16 (Federal Requirements to Protect Individual rights in State Unemployment Compensation Overpayment Prevention and Recovery Procedures) and UIPL No. 1-16, Change 1.

**Security Testing:**

The IDH and associated applications transmit and process sensitive UI claimant data, including Personally Identifiable Information (PII). To fully protect sensitive data, CESER has implemented a comprehensive information security approach including security policies, procedures, and tools. The IDH was developed in accordance with the Federal Information Security Management Act (FISMA) and NIST Special Publication 800-60 and has a security classification of “Moderate”. With this classification, the IDH follows the corresponding minimum-security controls, processes, and protocols specified in NIST Special Publication 800-53.

As a critical part of the comprehensive security approach, CESER has contracted with a specialized data security consulting firm to conduct penetration testing on the IDH. Penetration testing is an authorized simulated attack on a computer system, performed to evaluate and improve the security of the system. As part of some testing processes, security testers will be given temporary access to the IDH and, as such, will have visibility to sensitive state-owned information.

To ensure the integrity of the testing process, CESER shall:

- Fully vet any authorized contractor selected to conduct security testing;
- Execute a Non-Disclosure Agreement (NDA) that requires compliance with 20 CFR 603 and expressly prohibits the sharing of sensitive or confidential data, as well as security techniques employed by the IDH;
- Limit access of security testers to sensitive data to the minimum required to support testing; and
- Verify that temporary application access and visibility to the system provided to testers is revoked immediately upon conclusion of testing.

Penetration testing is a critical element of CESER's comprehensive security approach to identify and safeguard against any system vulnerabilities now, and in the future. Periodic ongoing security testing is planned in concert with ongoing internal security assessments.

## **Application, Architecture, and Development Support:**

The IDH has been developed using an open architecture and database application that can be expanded, as needed, to accommodate increased information collection, and processing, associated with the addition of participating states and providing expanded capabilities. To ensure the IDH architecture can adequately meet user's needs, CESER intends to use internal developers and specialized IT contractors to provide periodic application, development, and architecture support. Support elements may include, but not be limited to: application/database monitoring, technical architecture, database development and assessments, troubleshooting, and architecture/database optimization. As part of some support activities, support personnel will be given temporary access to the IDH and, as such, will have visibility to sensitive state-owned information.

To ensure the integrity of application and architecture support activities, CESER shall:

- Fully vet any authorized Contractor selected to provide application, development, and/or architecture support;
- Execute a Non-Disclosure Agreement (NDA) that requires compliance with 20 CFR 603 and expressly prohibits the sharing of sensitive or confidential data/practices;
- Limit access of support personnel to sensitive data to the minimum required to provide support; and
- Verify that temporary access and visibility to the system provided to support personnel is revoked upon conclusion of support activities.

**Disputes:** In the event of a dispute concerning the terms and conditions of this Agreement, or any order thereunder, which cannot be resolved by mutual agreement between the parties, either party to this Agreement may pursue any right or remedy it may have at law or in equity in any court of competent jurisdiction, or, if both parties agree, submit the dispute to the American Arbitration



Association for arbitration subject to/if permissible by applicable state law or policy.

**Independent Parties:** Nothing contained in this Agreement shall be deemed or construed to create a partnership or joint venture, to create relationships of an employer-employee or principal-agent, or to otherwise create any liability for one party whatsoever with respect to the indebtedness, liabilities, and obligations of the other party except as expressly provided herein.

**Public Information Releases:** State release of general public information concerning the activities conducted under this Agreement shall be coordinated with and approved by CESER.

**Entire Agreement:** This Agreement, composed of this document, all other documents incorporated by reference herein and any amendments executed in accordance with this paragraph, contains the entire understanding of the parties relating to the subject matter contained herein. No amendment or modification of any provision of this Agreement will be effective unless set forth in a document that purports to amend this Agreement and is executed by all parties.

**Severability:** If any terms or conditions of this Agreement are held to be invalid or unenforceable as a matter of law, the other terms and conditions shall not be affected, and shall remain in full force and effect.

**Non-Waiver:** The failure of the CESER to exercise any right or to require strict performance of any provision of this Agreement will not waive or diminish CESER's right thereafter to exercise such right or to require strict performance of any provision.

**Non-assignment:** State may not assign this Agreement, its obligations, or any interest hereunder, without the express prior written consent of CESER and NASWA. Any assignment made without consent shall be null and void and may constitute grounds for immediate termination of this Agreement by CESER.

**Liability:** States have various laws and constitutional restrictions regarding state liability related to contracts and agreements. Subject to such laws and restrictions, a party to this Agreement may be liable to another party to this Agreement only for the acts and omissions of its own employees and contractors, and only to the extent allowed or permitted by applicable state law.

**Integrity Data Hub (IDH) Participation Agreement**

Version: 5.0  
Date: 04/11/2022

By signing below, the signatories agree to bind their respective agencies/entities to the terms and conditions of this Agreement.

**U.S Virgin Islands Department of Labor**

By:

Signature: 

Name: Gary Molloy

Title: Commissioner

Date: 07/26/2022

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

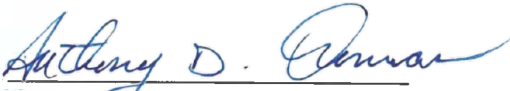
By:

Signature: 

Name: Scott B. Sanders

Title: President and CEO

Date: Jul 22, 2022



*MKT* Anthony D. Thomas Approve  
Commissioner  
Date: 8/16/2022

\_\_\_\_\_  
Anthony D. Thomas Disapprove  
Commissioner

APPROVED AS TO LEGAL SUFFICIENCY  
DEPARTMENT OF JUSTICE BY:  DATE 08/16/2022