**DOUGLAS R. HOFFER**
**STATE AUDITOR**

**STATE OF VERMONT**
**OFFICE OF THE STATE AUDITOR**

8 March 2022

The Honorable Phil Scott
Governor

Dear Governor Scott:

I am transmitting the second of two performance audit reports you requested regarding the Vermont Department of Labor (VDOL).[1] This report, conducted by the audit firm of CliftonLarsonAllen, LLP (CLA) focuses on DOL's processes and procedures used in the protection of personally identifiable information (PII). This topic is critical for all persons who submit such information to the VDOL since poor PII protection can result in identity theft and other bad consequences for individuals and the State.

This publicly available report contains five findings:

- VDOL should establish, through documented policies and procedures, a comprehensive program to protect the confidentiality of PII.
- Documentation of the PII data flow for all inbound and outbound interconnections, integrations and/or interfaces that transmit PII needs to be established.
- An inventory of all locations that store PII should be developed and maintained.
- VDOL should conduct privacy impact assessments and implement safeguards commensurate with the impact levels.
- Training should be provided regarding the proper handling of PII, including role-specific training as appropriate.

CLA is issuing a confidential report to VDOL that includes a sixth finding that contains sensitive security information.

As you will see in VDOL's response to a draft of this report, the Department plans to take action in response to CLA's recommendations. VDOL's response did not contain specific timelines for completion of these actions. While we plan to contact VDOL as part of our recommendation follow-up process next year, we strongly urge your Administration and the General Assembly to request specific timelines for the completion of corrective actions and to hold the Department accountable for meeting these deadlines.

[1] The first report was issued on April 22, 2021 and focused on VDOL's 1099G issuance process.

Please call or email me  if you have any questions.

Sincerely,

Doug Hoffer

Doug Hoffer
Vermont State Auditor

cc: The Honorable Jill Krowinski, Speaker of the House of Representatives
The Honorable Becca Balint, President Pro Tempore of the Senate
Mr. Adam Greshin, Commissioner, Department of Finance & Management
Rep. Michael Marcotte, Chair, House Committee on Commerce and Economic Development
Sen. Michael Sirotkin, Chair, Senate Committee on Economic Development, Housing and General Affairs
Mr. Michael Harrington, Commissioner, Department of Labor
Kristin Clouser, Secretary, Agency of Administration
Cameron Wood, Director, Unemployment Insurance

# STATE OF VERMONT
## Department of Labor

# PERFORMANCE AUDIT REPORT – PROTECTION OF PERSONALLY IDENTIFIABLE INFORMATION
## MARCH 2, 2022

WEALTH ADVISORY | OUTSOURCING
AUDIT, TAX, AND CONSULTING

CLAconnect.com

# VERMONT DEPARTMENT OF LABOR
## TABLE OF CONTENTS

# INDEPENDENT AUDITORS' REPORT AND EXECUTIVE SUMMARY

State of Vermont
Office of the State Auditor

CliftonLarsonAllen LLP (CLA) was engaged by the Vermont Auditor of Accounts to conduct a Performance Audit of the Vermont Department of Labor (VDOL) processes and procedures used in the protection of personally identifiable information. The purpose of this report is to provide findings and recommendations, which included identifying opportunities for VDOL to make long-term improvements to its internal control and quality assurance processes regarding the collection, use, storage, dissemination, and safe destruction of personally identifiable information(PII)[1]. Audit scope included an examination of the UI and Supplemental UI claims processing, including the controls around the collection, use and storage of electronic PII in the primary systems of record used in initial and ongoing claims. The audit was conducted in accordance with *Government Auditing Standards* issued by the Comptroller General of the United States.

We performed procedures from September to October 2021 to evaluate controls regarding access, classification, tracking and protecting PII; and to provide recommendations based upon best practices and other criteria, as applicable. Our findings are summarized as follows:

| Finding # | Finding |
|---|---|
| 1 | VDOL should establish, through documented policies and procedures, a comprehensive program to protect the confidentiality of PII. |
| 2 | Documentation of the PII data flow for all inbound and outbound interconnections, integrations and/or interfaces that transmit PII needs to be established. |
| 3 | An inventory of all locations that store PII should be developed and maintained. |
| 4 | VDOL should conduct privacy impact assessments and implement safeguards commensurate with the impact levels. |
| 5 | Training should be provided regarding the proper handling of PII, including role-specific training as appropriate. |

[1] Personally Identifiable Information (PII) is defined in 9 VSA §2430 (10)(A), and includes a consumer's first name or first initial and last name in combination with one or more of the following digital data elements: (i) a Social Security number; (ii) a driver license or nondriver State identification card number, individual taxpayer identification number, passport number, military identification card number, or other identification number that originates from a government identification document that is commonly used to verify identity for a commercial transaction; (iii) a financial account number or credit or debit card number, if the number could be used without additional identifying information, access codes, or passwords; (iv) a password, personal identification number, or other access code for a financial account; (statutory definition includes additional biometric, genetic and health information which is omitted from this footnote).

Due to the sensitive nature of computer security information related to these findings, specific information that may convey weaknesses in VDOL systems has been omitted from this report.

The responses from VDOL are included after each finding in the findings, recommendations, and management's responses section.

CliftonLarsonAllen LLP

**CliftonLarsonAllen LLP**
Baltimore, Maryland
March 2, 2022

## BACKGROUND

The Vermont Auditor of Accounts engaged CliftonLarsonAllen LLP (CLA) to conduct a Performance Audit of the Vermont Department of Labor ("VDOL") to identify opportunities to make long-term improvements to its internal control and quality assurance processes regarding the collection, use, storage, dissemination, and safe destruction of personally identifiable information related to initial and ongoing claims in the Unemployment Insurance and Supplemental Insurance Programs.

This Performance Audit was initiated as a complementary audit[2] related to performance audit of an incident in early 2021, wherein the Department mailed thousands of 1099G tax documents in which the name, mailing address, and/or social security number did not match the recipient.

## OBJECTIVES, SCOPE AND METHODOLOGY

We conducted this performance audit in accordance with Generally Accepted Government Auditing Standards (GAGAS) established by the U.S. Government Accountability Office (GAO). Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on the audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusion based on the audit objectives. Because of the inherent limitations, a performance audit made for the limited purposes of our review would not necessarily disclose all weaknesses related to the Vermont Department of Labor.

The objective of the audit was as follows:

- To identify recommendations and control improvements for Labor's unemployment insurance program to consider within its internal control and quality assurance processes regarding the collection, storage and retention, dissemination and transmission, and destruction or removal of personally identifiable information (PII).

Procedures Performed:

1) Examined the types of information gathered by VDOL during the initial and ongoing claims process, and the policies and procedures guiding the protection of PII in VDOL systems.
2) Through inquiry and observation, conducted an examination of the UI and Supplemental UI claims processing, including the controls around the collection, use and storage of electronic PII in the primary systems of record (VABS, Salesforce, Claimant Portal) used in initial and ongoing claims.
3) Through walkthroughs, inquiry and observation, evaluated controls related to authentication and access controls, encryption and data classification and handling and provide recommendations to improve according to best practices.
4) Compiled recommendations, as appropriate regarding other best practices in classifying, tracking, and protecting electronic data in primary and other ancillary systems as that were identified in the course of evaluating the UI systems used for initial and ongoing claims.

We conducted audit procedures with VDOL staff and managers responsible for the UI and Supplemental UI programs, which included Vermont Agency of Digital Services (ADS) information technology personnel responsible for the support and maintenance of VDOL systems. While the primary objective was to identify opportunities for improvement, auditors noted that generally sound controls were in place around user authentication and access, and encryption were present in the primary systems of record (VABS, Salesforce, Claimant Portal) that were observed.

[2] A Performance Audit Report related to the Department of Labor's Error in Distribution of Forms 1099G can be found at: https://auditor.vermont.gov/sites/auditor/files/documents/CLA%20DOL%20Performance%20Audit%20Obj%201.pdf

## FINDINGS, RECOMMENDATIONS AND MANAGEMENT'S RESPONSES

We identified areas for improvement related to the objectives of this audit. These items are discussed below and include our recommendations, together with the Department's responses.

### FINDING NO. 1 –

### DEVELOP POLICIES AND PROCEDURES REGARDING THE PROTECTION OF PII

**VDOL should establish, through documented policies and procedures, a comprehensive program to protect the confidentiality of PII.**

Various types of PII are collected in VDOL systems during the processing of initial UI claims. The most sensitive of which include primary identifiers such as Social Security Number, Alien Registration Number (if not a U.S. citizen), Driver's License Number, and financial information such as banking account information for direct deposit. Per inquiry with management, nearly all VDOL employees require access to claimant records that include PII to conduct day-to-day activities. Access to data is generally restricted in the VABS system, department-level file shares, and other systems that interface with the VABS system. The department relies heavily on the culture of trust instilled in its employees to protect PII, and has developed minimum guidance for employees for the protection of PII, but has not established a comprehensive set of policies, procedures, and other guidance specific to the protection of PII.

The dynamic resulting from the COVID-19 pandemic, which increased UI claimants and supplemental UI programs, has increased the volume of claimant data collected and the number of locations that contain it, and when combined with the pervasiveness of remote access by VDOL employees has increased the complexity of protecting PII data throughout the VDOL environment. PII data now resides in more areas in greater volume, and in some instances during the pandemic, has extended beyond the physical boundaries of the department into a telework environment. The volume of PII data collected by VDOL presents an attractive target for malicious cyber attackers, and pervasiveness of its use requires a comprehensive strategy to ensure proper protection and reduce the likelihood of a data breach.

VDOL can better manage this risk by establishing a program, policies and procedures to protect the confidentiality of PII. The National Institutes of Standards and Technology (NIST) publishes a Guide to Protecting the Confidentiality of Personally Identifiable Information, known as NIST Special Publication 800-122 (NIST SP800-122). The guide outlines best practices in protecting PII, and includes a structure and framework for managing risks, to the confidentiality of PII, suggesting that among many best practices, organizations should:

- Identify all PII residing in their environment.
- Minimize the use, collection, and retention of PII to what is strictly necessary to accomplish their business purpose and mission.
- Categorize their PII by the PII confidentiality impact level.
- Apply the appropriate safeguards for PII based on the PII confidentiality impact level.

### RECOMMENDATION(S)

1.1 We recommend VDOL further develop and document a comprehensive set of policies and procedures to guide the protection of PII throughout its environment and consider aligning those policies and procedure with the guidelines included in NIST SP800-122.

1.2 We recommend VDOL establish procedures and protocols for the security of PII data that needs to be taken offsite. Consideration should be given to the following:

- Establishing minimum physical security requirements for the protection of PII data at-home.
- Establishing procedures for tracking the chain of custody for PII data.
- Establishing guidance regarding the secure destruction of PII data.

***Management's Response***

As mentioned in the report, the Department of Labor has documented policies and procedures related to the protection and security of confidential information maintained by the Department. The Department recognizes that our current policies and procedures should be updated to the standards identified by CLA during this performance audit and should include protocols for protecting sensitive information given the changes to our work environments in response to the COVID-19 global pandemic, such as increased remote work options. The Department is committed to further developing a comprehensive program for the protection of the information entrusted to our care and will continue to update our policies and procedures moving forward.

## FINDING NO. 2 –

## DOCUMENT THE FLOW OF PII THROUGH VDOL AND EXTERNAL SYSTEMS

**Documentation of the PII data flow for all inbound and outbound interconnections, integrations and/or interfaces that transmit PII needs to be established.**

The system of record for UI, VABS, is a legacy mainframe application with a complicated system of routine inbound and outbound interconnections, integrations and/or interfaces (hereinafter, interfaces). Through processing initial and ongoing claims, we observed that PII data is received from or transferred to other systems that are internal to VDOL, other state agencies, and external organizations such as National Association of State Workforce Agencies' (NASWA) Integrity Data Hub (for fraud detection).

We performed walkthroughs of interfaces with four systems (Salesforce, NASWA's Identity Data Hub, VABS, Claimant Portal) used just in the entry of claimant information that results in the processing of a claimant's initial weekly claim. While the scope of this audit did not extend to external systems, we supplemented interviews with inspection of presentation materials from ADS dated June 16, 2021 depicting an Unemployment Insurance Systems Modernization initiative, including a high-level system map, which provided some context to the extent of system interfaces. Inspections concluded that there are 15 or more additional systems internal to the state, and 10 or more customer-facing systems that could potentially include PII data from claimants.

Per inquiry with ADS technology personnel regarding the general methods used for outbound systems interfaces include an extraction or export from VABS to a text file, a script that transforms the text file and loads it into a SQL server database dedicated to that interface, extractions from the database into the file/formats required by the destination system, and then transport through either an application program interface (API) or a secure file transport (SFTP) site that the source application can read. Inbound interfaces operate in a similar manner but may have fewer steps.

The result is a potential risk that each interface that transmits PII data could result in multiple (potentially two-to-five) copies of data files that may also contain PII. Each copy would need to be known and identified in order to be protected. Per VDOL and ADS, comprehensive documentation depicting the flow of PII data through its systems has not been created or maintained.

The first step toward controlling the confidentiality of PII information is understanding the inflows and outflows of data. NIST SP800-122 outlines the importance of identifying all PII data residing in your environment. Guidance further states “An organization cannot properly protect PII it does not know about.”

**RECOMMENDATION(S)**

1.1 We recommend VDOL collaborate with ADS to document the flow of PII data in its environment and through interconnected systems. Documentation should include data flow diagrams or other documentation to identify inbound and outbound interfaces and systems integrations that transmit PII data.

***Management’s Response***

The Department acknowledges and agrees with this finding. As part of the ongoing need to further develop and enhance our program to protect the confidentiality of PII (see Finding Number One), the Department will work with our Agency of Digital Services (ADS) partners to document PII data flows across our platform. The Department must balance this effort with our current resource availability given that the State is in the beginning stages of a massive whole system modernization effort to replace the current UI information technology infrastructure. A comprehensive documentation of PII data flows will be included as part of our modernization efforts for our new information technology systems.

## FINDING NO. 3 –

## INVENTORY PII STORAGE LOCATIONS

**An inventory of all locations that store PII should be developed and maintained.**

In addition to potential storage locations of PII data through interfaces, auditor interviews and observations noted that routine data extractions and reporting processes occur to support other operational and back-office activities for various VDOL departments to support the UI program. Examples include performance measures, adjudication data, mailing statements, and EFT files to process payment of claims. These extractions and reports are run daily, weekly, monthly and quarterly and may result in a significant amount of data being stored in file storage or staging areas.

Procedures to extract data from VABS are similar to outbound systems interfaces and include an extraction or export from VABS to a text file, a script that transforms the text file and loads it into a SQL server database (e.g. reporting database or data warehouse), extractions from the database into the file/formats required by the report or destination system, and copies created into VDOL department file shares, as applicable. Additionally, PII may also be contained in hardcopy data that is obtained from a claimant and stored in an imaging system.

The result is a potential risk that each routine data extraction or reporting process that transmits PII data could result in multiple copies of data files that may also contain PII, stored in various formats at various lengths of time. Each copy would need to be known and identified in order to be protected. Per VDOL and ADS, comprehensive inventory of all PII data storage locations has not been created or maintained. Further, some archiving occurs on files in staging areas, and purging occurs in the claimant portal. However, it was unknown whether any other purging activities are conducted.

NIST SP800-122 outlines the importance of identifying all PII data residing in your environment as well as minimizing the use, collection, and retention of PII to what is strictly necessary to accomplish their business purpose and mission. Guidance further states, "The likelihood of harm caused by a breach involving PII is greatly reduced if an organization minimizes the amount of PII it uses, collects, and stores."

**RECOMMENDATION(S)**

3.1 We recommend that VDOL collaborate with ADS to develop an inventory of PII data storage locations. Documentation should include databases, file storage used for reporting, and temporary staging areas used for interfaces, extractions and interfaces. The inventory should also profile the type and volume of PII stored in each location, context of use and the retention period.

3.2 We recommend VDOL and ADS establish procedures to perform a periodic review of data storage locations, to purge or remove copies of PII data that is not needed as an official record in accordance with established record retention policies. Procedures should be performed annually at a minimum and include consideration for archiving or removing data that is not required to be retained pursuant to 1 V.S.A. § 317a, 3 V.S.A. § 117 or other federal requirements.

***Management's Response***

The Department acknowledges and agrees with this finding. As part of the ongoing need to further develop and enhance our program to protect the confidentiality of PII (see Finding Number One), the Department will work with our ADS partners to document an inventory of all locations that store PII across our platform. The Department must balance this effort with our current resource availability given that the State is in the beginning stages of a massive modernization effort to replace the current UI information technology infrastructure. A comprehensive inventory of all locations that store PII will be included as part of our modernization efforts for our new information technology systems.

## FINDING NO. 4 –

## CONDUCT PRIVACY IMPACT ASSESSMENTS AND IMPLEMENT MINIMUM SECURITY CONTROLS

**VDOL should conduct privacy impact assessments and implement safeguards commensurate with the impact levels.**

During interviews and walkthroughs of internal controls, auditors observed sound security practices in those in the primary systems of record that were included in the review of initial and ongoing claims (Salesforce, VABS, Claimant Portal). For example, user passwords and authentication requirements (including MFA for Salesforce), role-based access controls, encryption in-transit and at-rest, and periodic review of user access. As documented in previous findings, this audit also identified several additional potential data storage locations for PII including interfaces, extractions, staging areas and report output, which may need to be subjected to a similar level of technical and operational controls in order to adequately protect the confidentiality of PII.

NIST SP800-122 outlines the importance of protecting PII according to the impact it has on the organization and its customers. It further suggests that organizations should categorize their PII by the PII confidentiality impact level and apply appropriate safeguards for PII based on the PII confidentiality impact level. The PII confidentiality impact level (e.g. low, moderate, or high) can be used to indicate the potential harm that could result to the subject individuals and/or the organization if PII were inappropriately accessed, used, or disclosed.

Additional guidance is provided to organizations to evaluate PII to determine its PII confidentiality impact level, suggesting guiding factors and procedures to conduct privacy impact assessments, so that appropriate operational or technical security controls can be appropriately applied.

## RECOMMENDATION(S)

4.1 We recommend VDOL collaborate with ADS to establish procedures to conduct privacy/confidentiality impact assessments for systems that store and transmit PII data. Assessments should consider factors such as the potential impact of a data breach based upon the sensitivity and volume of PII data contained in each location. VDOL should consider implementing technical security safeguards commensurate with the potential impact and risk, to ensure confidentiality is maintained.

4.2 We recommend VDOL establish standard operational safeguards for each PII data storage location. Consideration should be given to the following:

- Designating data controllers / owners for all locations that store PII.
- Procedures to verify least privilege access controls implemented and enforced for all PII storage locations.
- Procedures for a periodic review of user access for all PII storage locations.
- Procedures for monitoring of access to systems and data.
- Procedures to strategically de-identifying information so that complete records are not extracted or PII is removed whenever not required.
- Procedures to verify data is protected with encryption at-rest.

### *Management's Response*

In December 2021, the State's contracted security vendor performed a vulnerability scan of the Department's customer facing portals. While this was not a full assessment as outlined above, this review provided the Department with input and information on how secure the portals are from attack vectors by malicious actors. All issues identified in the review were immediately remediated and shown to no longer be present. There were no outstanding issues once the review was complete.

As mentioned in the report, the auditors observed sound security practices in our primary systems of records; however, the Department is fully supportive of striving for best practices wherever feasible. Based on the current structure of the UI program, there are two key types of PII. The private information that resides within the technology platform, and the information that is maintained outside of the various IT systems. As previously mentioned, the State is moving forward with a whole-system modernization effort that will address most of the concerns with regards to safeguarding system specific PII. Concurrently, the Department is taking steps to strengthen its internal quality control efforts. The UI Division has hired an assistant director for quality control and fraud prevention who will oversee the quality standards of the UI Division, including the safeguarding of information. At the Department level, we have created a business administration office, which includes a business operations manager, an administrative services director, and a business project manager, who's specific duties include continuous improvement, quality control, and safeguarding information across the Department. The Department is committed to the continued protection of PII maintained by the Department and will explore the opportunity of having a full privacy impact assessment developed during our ongoing work with ADS as outlined in our response to Finding Two and Three.

## FINDING NO. 5 –

## TRAINING FOR EMPLOYEES THAT HANDLE PII

**Training should be provided regarding the proper handling of PII, including role-specific training as appropriate.**

Per inquiry with management, nearly all VDOL employees require access to claimant records that include PII to conduct day-to-day activities. The department relies heavily on the culture of trust instilled in its employees to protect PII. General training is provided to new employees on the protection claimant information. Employees are also provided annual cybersecurity training and security awareness training through ADS, provided by Security Mentor, Inc.; however, a comprehensive training program is not established that includes awareness of the specific risks related to PII to account for all potential locations, or role-specific training for individuals with higher levels of access to PII.

NIST SP800-122 outlines the importance of implementing a training plan as a key area of operational safeguards for the protection of PII. Guidance further states, "The goal of training is to build knowledge and skills that will enable staff to protect PII. To reduce the possibility that PII will be accessed, used, or disclosed inappropriately, all individuals that have been granted access to PII should receive appropriate training and, where applicable, specific role-based training." The guide provides additional foundational areas regarding topics to cover and points of focus.

### RECOMMENDATION(S)

5.1 We recommend that VDOL expand upon its training for the handling of PII. Training materials should define PII, handling procedures, role-specific training, and include at a minimum, materials for management, operational employees and technology employees.

### *Management's Response*

As mentioned in the report, the Department of Labor requires employees to go through security and protection of PII training annually. In addition, staff are required to complete security trainings mandated by the State's Agency of Administration. The Department has recently updated our internal annual security training to include more detailed information about PII security and it now includes fact-specific examples of how to protect PII that is relevant to our work at the Department.