



Privacy Impact Assessment

for the

Employment Verification and Unemployment Compensation

DHS Reference No. DHS/ALL/PIA-096

January 11, 2023



**Homeland
Security**



Abstract

The Department of Homeland Security (DHS) outsources administration of its Employment Verification (EV) and Unemployment Compensation (UC) business functions, currently Equifax Workforce Solutions (vendor), due to the Department's large number of current and former employees.¹ With respect to Employment Verification, current and former DHS employees pursuing contracts and services with mortgage lenders, consumer finance companies, prospective employers, and other entities typically require verification of their current or past employment. Regarding Unemployment Compensation, recently separated DHS employees seeking unemployment compensation need the Department to work with the states and territories where they reside to ensure they receive any payments to which they are entitled. DHS is conducting this Privacy Impact Assessment (PIA) because the systems that support its Employment Verification and Unemployment Compensation functions collect, use, store, and transmit personally identifiable information (PII) and sensitive personally identifiable information (SPII).

Overview

Background

The National Finance Center (NFC),² for many years, provided Employment Verification and Unemployment Compensation services to other executive agencies via a contract it maintained with a credit monitoring agency. In early 2019, NFC notified its customer agencies that it would not renew this contract and that they would be responsible for managing their own Employment Verification and Unemployment Compensation services. In response, DHS developed an enterprise-level contract to procure full-service Employment Verification and Unemployment Compensation administration. This contract covers DHS employment history storage and maintenance, employment verification services, social services verifications, Unemployment Compensation claims processing, Unemployment Compensation appeals administration, and Employment Verification and Unemployment Compensation management reports and reviews.

Employment Verification (EV)

Employers of all types are regularly called upon to verify employment and income details of past and current employees, and federal agencies are no different in this respect. Numerous situations call for EV, including lenders wanting to confirm the income of prospective customers when deciding whether and in what amount to extend loans, landlords wanting to confirm stable

¹ The term DHS employee as used in this Privacy Impact Assessment only includes U.S. Coast Guard (USCG) civilian employees and not military, Reserve, or auxiliary employees.

² NFC is a federal agency under the U.S. Department of Agriculture's (USDA) Office of the Chief Financial Officer. It provides HR, financial, and administrative services for agencies across the Federal Government. For more information about NFC and its services, see <https://www.nfc.usda.gov>.

and sufficient income of prospective tenants, and companies wanting to verify the work experience of employment candidates. DHS outsources this function to a third-party vendor with specific expertise in EV.

The data DHS's Employment Verification vendor relies on to verify past or current employment and income details comes from NFC's Payroll/Personnel System (PPS).³ The vendor receives this data into its Employment Verification system directly from NFC PPS via biweekly data feeds that align with the biweekly pay cycles of DHS employees. Lenders, prospective employers, landlords, and others with a legitimate interest in employment and income data ("verifiers") who are credentialed in the Employment Verification system can access an online portal to verify the employment and income details of current and former DHS employees seeking their services or support. The Employment Verification system also enables current and former DHS employees to access their own employment and income details, along with a full accounting of any fulfilled verifications, via a separate online portal. DHS can also use the system to manage what information about the agency employee is available to verifiers and review industry-level metrics related to verifications accessed by credentialed verifiers.

Verifiers

DHS's outsourced Employment Verification system provides verifiers with instant employment and income verifications to facilitate financial risk assessments and other service-related decisions. All verifiers are themselves verified by DHS's Employment Verification vendor to confirm they are a legitimate business with a legitimate need to know income, employment, or social services information in the normal course of their business activities—a process known as "credentialing." The Employment Verification vendor credentials all verifiers when they register an account in its Employment Verification system, and periodically thereafter, for as long as the verifier maintains the account.⁴

1. Verifier Registration

When a verifier registers an account in the Employment Verification system, DHS's Employment Verification vendor collects personally identifiable information and other business information to support the credentialing process and to set up the verifier's system profile. This includes collecting business contact information; name, job title, and contact information of the individual registering on the verifier's behalf; information about the verifier's industry type (e.g.,

³ NFC PPS is an integrated payroll/personnel processing system offering a full range of personnel and payroll processing. It processes personnel actions; awards; allotments; bonds; performance appraisals; health and health insurance; thrift savings plans; tax documents; severance pay; leave records; and payroll-related financial reporting operations. For more information, see NFC PPS Payroll Personnel System (PPS) PIA, available at <https://www.usda.gov/home/privacy-policy/privacy-impact-assessments>.

⁴ Verifiers are generally reverified annually; however, large, well-known, and well-established institutions like major banks may be reverified less frequently.



bank, mortgage lender, government agency); any relevant licensing information; the types of reports the verifier would collect (employment and income, employment only, or social services verification, as described below); and information about the business purposes for which the reports would be collected (“permissible purpose”). Justifiable permissible purposes are defined in Section 604 of the Fair Credit Reporting Act (FCRA),⁵ and include the following:

- In response to a court order or federal grand jury subpoena;
- In accordance with the written instructions of the Consumer to whom it relates; or
- To a verifier that the Employment Verification vendor has reason to believe intends to use the information for any of the following reasons:
 - In connection with a credit transaction involving the DHS employee on whom the information is to be provided and that involves (a) extending credit to the DHS employee, (b) reviewing an account of the DHS employee, or (c) collecting an account of the DHS employee;
 - For child support purposes, such as establishing an individual’s capacity to make child support payments or determining the appropriate level of such payments;
 - For employment purposes, subject to additional requirements described below;
 - In connection with the underwriting of insurance involving the DHS employee;
 - In connection with a determination of the DHS employee’s eligibility for a license or other benefit granted by a governmental instrumentality required by law to consider an applicant’s financial responsibility or status;
 - To a potential investor or servicer, or current insurer, in connection with the valuation or risk assessment or prepayment risks associated with, an existing credit obligation; or
 - Otherwise has a legitimate business need for the information, such as a business transaction initiated by the DHS employee; or to review an account to determine whether the DHS employee continues to meet the terms of the account.

⁵ The Fair Credit Reporting Act is federal legislation enacted to promote the accuracy, fairness, and privacy of consumer information contained in the files of consumer reporting agencies. It is intended to protect consumers from the willful or negligent inclusion of inaccurate information in their credit reports. To that end, the Fair Credit Reporting Act regulates the collection, dissemination, and use of consumer information, including consumer credit information. More information about the Fair Credit Reporting Act is available at <https://www.consumerfinance.gov/compliance/compliance-resources/other-applicable-requirements/fair-credit-reporting-act>.



Additionally, the verifier is required to certify the permissible purpose they are using for each verification they access.

Once this step is complete, the verifier receives an email to activate the account, and the verifier clicks on an activation link in the email to proceed.

Before completing the registration process, the verifier is required to read and agree to a disclosure and consent agreement,⁶ rights and duties specified in Fair Credit Reporting Act, and other terms and conditions.⁷ After acknowledging these agreements and registering the account, the verifier is prompted to log into the Employment Verification system with a username and password. However, the verifier is not able to use the system to retrieve DHS employee personally identifiable information until it is fully credentialed by Employment Verification system administrators.

2. Verifier Credentialing

Once a verifier registers an account, the credentialing process begins. This entails DHS's Employment Verification vendor using information submitted during the registration process to confirm the verifier is a legitimate business with a legitimate need for employment, income, or social services information about current or past DHS employees. Typical strategies for credentialing include:

- Checking that the domain name of the business email address collected during registration correlates with the customer's business name;
- Entering physical addresses provided by verifiers during the registration process into search engines and online mapping tools to determine whether the business appears at the specified location;
- Reviewing Secretary of State data to confirm the verifier is in good standing;
- Reviewing Office of Inspector General data to confirm the verifier qualifies to access Social Services Verifications;
- Conducting physical onsite inspections for verifiers that meet certain criteria to confirm the verifier has appropriate security controls in place;

⁶ The federal Electronic Signatures in Global and National Commerce Act (ESIGN) facilitates the use of electronic records and electronic signatures in interstate and foreign commerce by ensuring the validity and legal effects of contracts established electronically. Among other things, it preserves the rights of individuals to choose not to use electronic signatures and requires businesses to retain electronic records under specified criteria. More information about the federal Electronic Signatures in Global and National Commerce Act is available at <https://www.fdic.gov/regulations/compliance/manual/10/X-3.1.pdf>.

⁷ These other terms and conditions relate to licensing and copyright, and include limited liability disclaimers for unintentional data errors, system outages, and misuse of information by outside parties.



- If the verifier registers as a mortgage company, checking the Nationwide Multistate Licensing System & Registry (NMLS)⁸ database to validate the business is licensed as such;
- If the verifier registers as a bank, checking Federal Deposit Insurance Corporation (FDIC) records to validate the business is licensed as such; or
- If the verifier registers as a credit union, checking National Credit Union Administration (NCUA) records to validate the business is licensed as such.

If these sorts of activities establish that the verifier is indeed a legitimate business with a legitimate reliance on consumer employment, income, or social services data, Employment Verification system administrators enable the verifier to begin using the system to retrieve Employment Verification reports.⁹

3. Obtaining Employment Verification Reports

Credentialed verifiers request Employment Verification reports by first logging in to the Employment Verification system using a username and password. Verifiers then select the type of report they are seeking, which can be for verification of employment only (VOE report), verification of both employment and income (VOI report), or Social Services Verification (SSV report).¹⁰ Next, the verifier selects a permissible purpose for its report request from a dropdown menu. The verifier then enters the Social Security number (SSN) of the individual (which it already has from the information the individual submitted directly for Employment Verification services) and submits the request. Once submitted, the system immediately retrieves the relevant data from its database and the requested report is automatically generated.

Reports verifying only employment include employee name, employer name and address, dates of employment, job title, and pay frequency. Reports verifying both employment and income contain this same information plus income information by calendar year and by pay period for the entire length of employment. Social Services Verification reports include the information contained in verification of both employment and income reports as well as additional pay details and information related to benefits that the employee is receiving. All types of reports also include a report tracking number, a report creation date, and the date at which data in the report was last updated.

⁸ The Nationwide Multistate Licensing System & Registry is the sole system of licensure for mortgage companies for 58 state agencies and the sole system of licensure for mortgage loan originators for 59 state and territorial agencies.

⁹ A single verifier may have multiple users that may sign in on its behalf to retrieve reports, especially when the verifier is large and ubiquitous. In these cases, new users are only added to a verifier account once the Employment Verification vendor checks with an existing user to validate that the new user has a need-to-know employment and income data in the normal course of his or her job duties.

¹⁰ Verifiers purchase each report they obtain from the system from the Employment Verification vendor.



Credentialed verifiers may also retrieve reports they previously requested via the Employment Verification system's online portal for seven (7) days after purchase. Verifiers may search for these reports by reference number. Verifiers may also retrieve a list of their pending report requests using the same search criteria.

Employee Access to Employment Verification Information

The Employment Verification system also enables employees to access their own employment and income details, along with a full accounting of all fulfilled verifications pertaining to them in the last two (2) years. As with verifiers, employees must first create an account in the system. Account creation for employees involves submitting name, Social Security number, date of birth, personal email address, and a username and password. If the name, Social Security number, and date of birth match information already in the system that was collected from NFC PPS, the employee's account is approved.

After creating an account, employees can log into the system to access all information the Employment Verification vendor has pertaining to their past and current employment and income, including all current information that could be made available to verifiers who request verification of employment only, verification of both employment and income, or Social Services Verification reports about them. Employees can also generate reports about themselves which are marked as internal use only.

Employees can also use the Employment Verification system to view inquiry history for prior reports about them that have been provided to verifiers for the last two (2) years.¹¹ Additionally, employees can view and change their profile information, change their password, and restrict access by verifiers to their information.

DHS Access to the Employment Verification System

The Employment Verification system also contains a section specifically for employers that have contracted with the Employment Verification vendor. In the case of DHS, the section allows a limited number of DHS personnel who conduct Employment Verification-related operations as part of normal job duties (DHS administrators) to access Employment Verification data pertaining to other DHS employees. This data includes the types and content of any

¹¹ There are there are two sections of the FCRA that require credit reporting agencies to disclose information in credit reports without telling the consumer. Thus, employees would be unable to use the system to view these inquiries. One FCRA section requires credit reporting agencies to provide information in credit reports to the FBI for counterintelligence purposes. The other section requires credit reporting agencies to share credit report information with an appropriate government agency for counterintelligence purposes. These are not "credit checks," but credit reporting agencies are nonetheless forbidden from disclosing to the consumer that the information in the credit report was shared. *See* 15 U.S.C. § 1681u and 15 U.S.C. § 1681v.



Employment Verification reports verifiers requested concerning DHS employees.¹² The DHS employer's section also includes a dashboard displaying total number of DHS employee verification reports requested by government verifiers and commercial verifiers, the total number of reports DHS employees have generated about themselves, and the most recent date at which the Employment Verification vendor received a data feed from NFC PPS.

Unemployment Compensation (UC)

Since 1955, federal civilian employees have had unemployment insurance protection under US Code Title 5, Chapter 85. The Omnibus Reconciliation Act of 1980 (Pub. L. 96-499, December 5, 1980) amended Unemployment Compensation for federal employees by establishing the requirement that each federal agency contribute to state unemployment benefits on behalf of their employees.¹³ Thus, DHS is mandated to cover Unemployment Compensation claims for separated DHS employees, and employees placed in a nonpaid status, who qualify under the laws of their state or territory.

State Unemployment Compensation laws and policies vary significantly regarding eligibility requirements, payment amounts, and periods of eligibility. This makes it difficult for federal personnel who are not familiar with detailed state requirements to track unemployment benefit payments; ensure payments have been properly applied; and verify, review, and appeal claims within prescribed time limits. Consequently, DHS outsources most administrative functions related to Unemployment Compensation.¹⁴

Each of the 52 U.S. states and territories that manage an unemployment insurance program relies on a single system, the Unemployment Insurance Interstate Connection Network (ICON), to exchange data with federal agencies in the filing and processing of Unemployment Compensation claims submitted by federal workers residing in their jurisdiction. When a federal worker files an Unemployment Compensation claim, the state or territory provides submitted claim information to the employing federal agency, or their agent or contractor.¹⁵ In the case of DHS, these data transmissions of unemployment claims go directly to its Unemployment Compensation vendor via

¹² Unlike verifiers and employees, employers do not need to register for a system account or set up a profile since the Employment Verification vendor does this for them during the contracting phase or shortly thereafter. Specific information captured in the employer's profile is listed in Section 2.1.

¹³ 20 C.F.R. Part 609 sets forth the Secretary of the Department of Labor (DOL) regulations to implement federal Unemployment Compensation programs.

¹⁴ Although subject to change in the future, DHS currently uses the same Unemployment Compensation vendor that administers its Employment Verification function. Vendors with expertise in Employment Verification frequently also have expertise in Unemployment Compensation since these functions generally rely on the same type of data and require similar types of coordination with federal stakeholders.

¹⁵ States also use the Unemployment Insurance Interstate Connection Network to exchange Unemployment Compensation data with other states and federal agencies for such purposes as identifying whether a claimant has a claim or wages in another state, requesting assistance with collection efforts, and developing metrics regarding re-employment outcomes. For more information on the Unemployment Insurance Interstate Connection Network, *see* <https://www.naswa.org/icon>.



a direct integration between the vendor's Unemployment Compensation system and the Unemployment Insurance Interstate Connection Network.

DHS provides its workers who are separated from their jobs with Standard Form 8 - Notice to Federal Employees about Unemployment Insurance (SF-8), as well as a Standard Form 50 - Notification of Personnel Action (SF-50) that reflects the personnel action that resulted in their separation. The SF-8 lists the name and address of the employing agency, a telephone number for the agency's unemployment compensation program, and a 3-digit agency identification code. Instructions on the SF-8 advise recipients to submit it to the nearest local public employment services office if they would like to file an Unemployment Compensation claim.¹⁶ The SF-50 contains other information relevant to Unemployment Compensation claims such as reason for separation, salary and wages, job title, and duty location.

When claimants arrive at their local employment services office and provide the SF-8 as evidence of their recent federal employment, they are also required to submit whatever other information the laws of their state or territory require to initiate a claim. This typically includes demographic information, as well as information reflected on the SF-50 such as salary and wages, length of employment, type of employment, and reason for their separation or nonpaid status. As the state processes the claim, it enters the data submitted by the claimant into its unemployment insurance system, and thereafter the data gets transmitted through the Unemployment Insurance Interstate Connection Network to the employing federal agency.¹⁷

For claims directed at DHS, the Unemployment Compensation vendor retrieves the data transaction from the Unemployment Insurance Interstate Connection Network and stores it locally in the Unemployment Compensation system. The vendor then conducts an initial review of data related to the claimant and his or her employer to ensure completeness and applicability to DHS, and to assign the claim to the correct state unemployment insurance account and DHS Component. After this initial review, the Unemployment Compensation vendor responds to a set of data requests from the state in the form of open text fields and dropdown menus designed to elicit information directly relevant to benefits entitlement under the state's law (e.g., job title, dates of employment, reason for separation). Additionally, the Unemployment Compensation vendor responds to "wage audit" questions relating to compensation in the relevant employment period and benefit year since this informs the amount of benefit to which a claimant may be entitled.¹⁸ Once the Unemployment Compensation vendor enters this information in the Unemployment

¹⁶ Additionally, the form recommends that claimants who wish to expedite their claims bring their Social Security account number card, the official notice of their most recent separation or of their present nonpaid status (preferably an SF-50), and earnings and leave statements or similar documentation.

¹⁷ Data requested by states and territories of federal agencies is always the same regardless of claimant or agency. See Section 1.2 for specific data elements requested.

¹⁸ All information that the Unemployment Compensation vendor transmits back to the state comes from the biweekly data feed it receives from NFC PPS.



Insurance Interstate Connection Network, it is transmitted back to the state for a benefits determination.

As the state is evaluating the benefits determination, it will sometimes reach back to the Unemployment Compensation vendor to request human resources (HR) documentation substantiating the vendor's previous Unemployment Insurance Interstate Connection Network responses. Examples of documentation the state might request include proficiency and performance assessments, time and attendance records, and termination and downsizing notices. Upon receiving these requests from the state, the vendor contacts designated HR specialists in the DHS Component where the employee worked to collect the necessary documentation. Once received, the vendor provides it back to the state in accordance with defined time limits.

If the state determines the totality of the information from the Unemployment Compensation vendor demonstrates eligibility for Unemployment Compensation benefits, the state office records the result, registers an "initial decision" approving the claim, and notifies the claimant of their eligibility for benefits. Alternatively, the local office denies the claim, registers the denial as the initial decision, and notifies the claimant of their right to appeal. Like the claimant, DHS also has the right to appeal an initial decision, and the Unemployment Compensation vendor has set criteria in place with DHS for when an appeal is appropriate. Typically, the vendor will automatically appeal decisions to grant Unemployment Compensation claims to DHS employees who separated or are in a nonpaid status due to suspension, termination, removal, sabbatical, being placed in a leave without pay status, and resignation in lieu of involuntary separation.

Whether an appeal is initiated by the claimant or by DHS, the Unemployment Compensation vendor provides support to DHS throughout the appeals process. This includes preparing the relevant DHS Component to attend all hearings and to provide responses to all procedural questions and issues; ensuring all claim and appeal documentation is complete, accurate, timely, compliant with specific states' guidelines and laws; and providing review, witness preparation, and consultation services throughout the appeals process. The Unemployment Compensation vendor may also attend appeals hearings anywhere in the United States to provide additional support to DHS upon request.

Section 1.0 Authorities and Other Requirements

1.1 What specific legal authorities and/or agreements permit and define the collection of information by the project in question?

15 U.S.C. § 1681 The Fair Credit Reporting Act, as amended, regulates the way credit reporting agencies and other organizations may collect, access, and use data for purposes of assessing creditworthiness and other information on consumers.

The Omnibus Reconciliation Act of 1980 (Pub. L. 96-499, December 5, 1980) establishes



the requirement that each federal agency contribute to state unemployment benefits for former government employees.

20 C.F.R. Part 609 sets regulations for the Secretary of the Department of Labor to implement the Unemployment Compensation for Federal Employees (UCFE) program.

5 U.S.C. Chapter 85 establishes criteria and conditions between the Federal government and the States for the payment of unemployment compensation benefits to federal civilian employees and ex-servicemembers.

42 U.S.C. § 405(c)(2)(C)(i) permits any state, in the administration of any tax or public assistance, to utilize Social Security number for the purpose of establishing the identification of individuals affected by such administration.

1.2 What Privacy Act System of Records Notice(s) (SORN(s)) apply to the information?

Information collected, maintained, used, and disseminated by DHS and its Employment Verification and Unemployment Compensation vendor in support of employment verification and unemployment compensation services is covered by OPM/GOVT-1 General Personnel Records¹⁹ and by DHS/ALL-019 Payroll, Personnel and Time and Attendance Records.²⁰

1.3 Has a system security plan been completed for the information system(s) supporting the project?

The Employment Verification and Unemployment Compensation vendor system will be covered by the pending FedRAMP DHS Employment Verification and Unemployment Compensation System Security Plan. This plan will be continuously updated after initial publication to cover ongoing changes to the Employment Verification and Unemployment Compensation Program.

1.4 Does a records retention schedule approved by the National Archives and Records Administration (NARA) exist?

The National Archives and Records Administration (NARA) General Records Schedule (GRS) 2.0 Human Resources series covers all the categories of information contained in Employment Verification and Unemployment Compensation vendor systems that are sourced from NFC PPS, and all information it shares with verifiers, employers, employees, and state unemployment insurance offices. Specifically, the following General Records Schedule rules

¹⁹ See OPM/GOVT-1 General Personnel Records, 77 Fed. Reg. 73694 (December 11, 2012), as modified by 80 Fed. Reg. 74815 (November 30, 2015), available at <https://www.dhs.gov/system-records-notices-sorns>.

²⁰ See DHS/ALL-019 Payroll, Personnel and Time and Attendance Records, 80 Fed. Reg. 58283 (September 28, 2015), available at <https://www.dhs.gov/system-records-notices-sorns>.



apply:

- Employee Management Administration Records: GRS. 2.2, item 010 (DAA-GRS-2017-0007-0001).
- Official Personnel Folder (OPF)/electronic OPN (eOPF) Short-term Records: GRS 2.2, item 041 (DAA-GRS-2017-0007-0005)
- Notifications of Personnel Actions: GRS 2.2, item 050 (DAA-GRS-2017-0007-0006).
- Records Used to Calculate Payroll, Arrange Paycheck Deposit, and Change Previously Issued Paychecks: GRS 2.4, item 010 (DAA-GRS-2019-0004-0001)
- Time and Attendance Records: GRS 2.4, item 030 (DAA-GRS-2019-0004-0002)
- Separation Program Management Records; Records Not Specific to an Agency Separation Initiative: GRS 2.5, item 010 (DAA-GRS-2014-0004-0001)
- Separation Program Management Records; Records Specific to an Agency Initiative Such as Reduction-In-Force, Voluntary Early Retirement, Voluntary Separation, and Similar Programs: GRS 2.5, item 011 (DAA-GRS-2014-0004-0002)
- Individual Employee Separation Case Files: GRS. 2.5, item 020 (DAA-GRS-2014-0004-0003)

1.5 If the information is covered by the Paperwork Reduction Act (PRA), provide the OMB Control number and the agency number for the collection. If there are multiple forms, include a list in an appendix.

Employment verification and unemployment compensation data is not covered by the Paperwork Reduction Act because it is collected from employees during their employment at DHS and not from the general public.

Section 2.0 Characterization of the Information

2.1 Identify the information the project collects, uses, disseminates, or maintains.

The Employment Verification and Unemployment Compensation vendor receives a biweekly data transmission from NFC PPS containing the following data for every DHS employee:

- Employee Information



- Employer Company Code
- Employee Social Security Number
- Employee PIN
- Adjusted Hire Date
- Employee Identifiers
 - Employee Last Name
 - Employee First Name
 - Employer Division / Location Code
 - Employee Address
 - As of Date
 - Job Title / Current Position
 - Employee Status Code
 - Most Recent Hire Date
 - Date of Termination / Inactivity / Retirement
- Salary Information
 - Employee's Current Pay Rate
 - Employee's Current Pay Rate Description Code
 - Totals for Current Year-To-Date
 - Gross Base Pay Amount
 - Gross Overtime Amount
 - Gross Bonus Compensation
 - Gross Commissions Amount
 - Total Gross Amount
 - Totals for Previous Year
 - Gross Base Pay Amount
 - Gross Overtime Amount
 - Gross Bonus Compensation
 - Total Gross Amount



- Totals for Year Previous to Last Year
 - Gross Base Pay Amount
 - Gross Overtime Amount
 - Gross Bonus Compensation
 - Total Gross Amount
- Social Services Data
 - Current Pay Period Ending Date (last 12 Pay Periods)
 - Current Pay Date (last 12 Pay Periods)
 - Hours Worked for Current Pay Period (last 12 Pay Periods)
 - Current Pay Period Gross Earnings (last 12 Pay Periods)

When a verifier registers an account in the Employment Verification system, the verifier provides the vendor the following information as part of the registration process:

- First Name
- Last Name
- Work Email
- Work Telephone
- Company Name
- Years in Business
- Other Business Name
- Federal Tax ID
- Physical Address (Street, City, State, Zip)
- Business Telephone
- Company Website
- Business License Issuer
- Department
- License Number
- Business Structure



- Stock Ticker
- Industry
- Nature of Business
- Permissible Purpose
 - Eligibility for government benefit
 - Extension of a firm offer of credit
 - For a legitimate business need tied to a consumer-initiated transaction other than credit decisions
 - For employment purposes
 - In connection with credit transaction(s) involving a consumer extension of credit including mortgage
 - Non-regulatory option-no permissible purpose required
 - Potential investor or servicer, or current issuer of existing credit obligation
 - To assess consumers' continued actions required under terms of existing account obligations including account review
 - Underwriting of insurance

Credentialed verifiers submit the following information into the Employment Verification system when retrieving verification of employment only reports and verification of both employment and income reports:

- Username and Password
- Type of Report Requested
- Permissible Purpose
- Social Security Number

Verification of employment only reports contain the following data fields:

- First Name
- Last Name
- Social Security Number
- Employer Name and Employer ID
- Current as of Date

- Date of Verification
- Reference Number
- Employer Address (Street, City, State, Zip)
- Division
- Job Title
- Employment Status
- Most Recent Start Date
- Original Hire Date
- Total Time with Employer

Verification of both employment and income reports contain the same data fields as verification of employment only reports, plus the following:

- Employee Rate of Pay
- Employee Pay Frequency
- Average Hours Worked / Pay Period
- Pay Cycle
- Last Amount of Pay Increase
- Last Date of Pay Increase
- Next Amount of Pay Increase
- Next Date of Pay Increase
- Annual Income Summary²¹
 - Year
 - Base Salary
 - Overtime
 - Commission
 - Bonus

²¹ This category of pay data is broken out by calendar year.



- Other²²
- Total

Social Services Verifications reports contain the same data fields as verification of both employment and income reports, plus the following:

- Benefits
 - Medical
 - Dental
 - Vision
- Worker's Compensation
 - Receiving Worker's Compensation
 - Carrier
 - Date of Injury
 - Date of Award
 - Claim Number
 - Claim Pending
- Payroll Deduction for All Insurance Coverage
- Pay Period Detail
 - Income
 - Total Gross Earnings
 - Total Net Earnings
 - Pension
 - Other Income
 - Withholding
 - Federal Tax
 - State Tax
 - Local Tax

²² Wages categorized as "other" may include vacation buyout, military pay, comp time, holiday pay, sick time, personal time, and/or sabbatical pay.



- Social Security
 - Medicare
 - Retirement/401k
 - Cafeteria Plan
 - Garnishments
 - Other Withholding
- Historical Pay Period Summary

Employers may choose not to share certain information reflected by any of the data fields in verification of employment only, verification of both employment and income, or Social Services Verifications reports when configuring their profiles. In these cases, the data fields are designated with N/A in the reports received by verifiers.

When an employee creates an account in the Employment Verification system, the vendor collects the following information as part of the registration process:

- Employer Code
- First Name
- Last Name
- Social Security Number
- Date of Birth
- Home Address (Street, City, State, Zip, Country)
- Personal Phone
- Email Address

The employee can view all information in the Employment Verification system that a current or past employer has provided to the Employment Verification vendor and that is included in their Employment Data Report. The Employment Data Report contains the same information as the verification of employment only, verification of both employment and income, and Social Services Verifications reports.

The following information is contained in employee profiles visible within the Employment Verification system:

- First Name
- Last Name



- Last 4 Social Security Number
- Date of Birth
- Phone (work, mobile)
- Email (work, personal)

The following Unemployment Compensation claims information is provided to the Unemployment Compensation vendor when claims are initiated:

- Claimant Name (first, last)
- Claimant Social Security Number
- Claimant's Job Title
- First Day Claimant Reported to Work
- Last Day Claimant Reported to Work
- Claimant Provided Reason for Separation (includes comments)
- Claimant's Return to Work Date (if applicable)
- Employer Federal Employment ID (FEIN)
- State Unemployment Insurance Account Number
- State Unemployment Insurance Office Name and Phone

When a claim is filed, the Unemployment Compensation vendor responds to a set of data requests, fulfilled in the form of blanks and dropdown menus, that includes:

- Claimant Job Title
- Seasonal Worker (Y/N)
- First Day of Work
- Last Day of Work
- Date of Separation (if different from last day of work)
- Employee Separation Reason
 - Permanent Layoff
 - Temporary Layoff or Furlough
 - Quit
 - Discharged



- Labor Dispute
- Retirement
- Other
- Employee Current Pay Rate
- Employee Current Pay Rate Description Code (e.g., annual, biweekly)
- Gross Pay Amount (year to date, last year, two years past)
- Gross Overtime Amount (year to date, last year, two years past)
- Gross Bonus Compensation (year to date, last year, two years past)
- Gross Commissions Amount (year to date, last year, two years past)
- Gross Other Income Amount (year to date, last year, two years past)
- Total Gross Amount (year to date, last year, two years past)

2.2 What are the sources of the information and how is the information collected for the project?

The sources of information for DHS's Employment Verification and Unemployment Compensation functions are those described in Section 2.1, and include the biweekly data feeds from NFC, data collected from verifiers and employers when registering accounts in the Employment Verification and Unemployment Compensation vendor systems, additional information collected from verifiers during the credentialing process, and information received from the state related to Unemployment Compensation claims submissions. The Employment Verification and Unemployment Compensation vendor may also collect HR information and documentation from DHS Components on an ad hoc basis to support Employment Verification and Unemployment Compensation operations.

2.3 Does the project use information from commercial sources or publicly available data? If so, explain why and how this information is used.

No. All data collected, used, shared, and stored by DHS and its Employment Verification and Unemployment Compensation vendor in support of Employment Verification and Unemployment Compensation operations comes from either government data sources that are not accessible to the general public or from the individuals themselves.



2.4 Discuss how accuracy of the data is ensured.

Data from NFC PPS is provided to the Employment Verification and Unemployment Compensation vendor via an automated feed with no human intervention, so data collected is the same as that used by NFC to calculate payroll, benefits, and other essential HR functions for DHS employees. The Employment Verification and Unemployment Compensation vendor systems also regularly conduct automated checks of data quality to ensure no duplicate data and to ensure the information received makes logical sense in the context of the subject and function to which it refers. Data provided to states via the Unemployment Insurance Interstate Connection Network is directly uploaded from the Employment Verification and Unemployment Compensation vendor system database, and copies of HR documents requested by states are sent by regular mail rather than electronically transcribed. Additionally, employees can access their own information at any time using the Employment Verification and Unemployment Compensation system to verify accuracy. They can also access their NFC data via other means such as their MyEPP account,²³ eOPF file,²⁴ and by submitting Privacy Act and Freedom of Information Act (FOIA) requests.

2.5 Privacy Impact Analysis: Related to Characterization of the Information

Privacy Risk: There is a risk that the Employment Verification and Unemployment Compensation vendor will collect more information about DHS employees than is needed for management of Employment Verification and Unemployment Compensation operations.

Mitigation: This risk is partially mitigated. The Employment Verification and Unemployment Compensation vendor only collects data from NFC PPS that could potentially become relevant during a verification of employment or a claim for unemployment compensation. It is difficult to know in advance what type of HR-related data might be relevant in a specific case, but only information that could potentially become relevant is included in the data feed from NFC. The Employment Verification and Unemployment Compensation vendor uses standard file formats for collecting employment and income information from NFC PPS.

Privacy Risk: There is a risk that the Employment Verification and Unemployment Compensation vendor database will contain inaccurate data due to the latency of data transfers from NFC PPS.

²³ See <https://www.nfc.usda.gov/EPPS>.

²⁴ A federal employee's Official Personnel Folder (OPF) contains all the official records required to document his or her career. The Electronic OPF (eOPF) is an electronic version of the OPF used by the vast majority of federal agencies and a system managed by the Office of Personnel Management (OPM) for accessing the electronic folder online. For more information regarding eOPF and its privacy implications, see OPM's eOPF Privacy Impact Assessment, available at <https://www.opm.gov/information-management/privacy-policy/privacy-policy/eopf-pia.pdf>.



Mitigation: This risk is partially mitigated. For current employees, the biweekly data feeds from NFC are added to the record from the prior transmission, so a complete history of employee data will be contained in the record going back as far as seven years. Thus, any change to personnel data will be updated in the Employment Verification and Unemployment Compensation vendor database within two weeks' time. In the rare instance a change in data that could impact an Employment Verification or Unemployment Compensation decision occurs between the time data is updated in NFC PPS and the time the Employment Verification and Unemployment Compensation vendor receives it, the employee can seek redress in the Employment Verification and Unemployment Compensation system by emailing the Employment Verification and Unemployment Compensation vendor support team at an email address prominently displayed on the landing page. If Unemployment Compensation claims submission data is filed with the state that does not match NFC data due to latency issues, the employee may contact any HR specialist that services his or her duty location to collect the correct information and provide it to the state.²⁵ Unemployment Compensation claimants may also request that the state seek the specific HR documentation that reflects the current data from DHS, or they can appeal initial claims decisions if a denial of benefits is based on outdated information. Additionally, under the Fair Credit Reporting Act, DHS is required to assure maximum possible accuracy for data furnished to the Employment Verification and Unemployment Compensation vendor.

Privacy Risk: There is a risk that verifiers may be able to access information about DHS employees in the Employment Verification system they do not need for purposes of verifying income or employment.

Mitigation: This is partially mitigated. Verifiers are credentialed during the process of establishing their Employment Verification system accounts to ensure they are a legitimate business with a legitimate need for employment and income information from DHS employees. Assuming they are successfully credentialed, they only receive the data listed in Section 2.1 for verification of employment only, verification of both employment and income, or Social Services Verifications reports. Some of the information provided in these reports may not be needed for purposes of a specific verification; thus, no additional information is provided.

Section 3.0 Uses of the Information

3.1 Describe how and why the project uses the information.

DHS's Employment Verification and Unemployment Compensation vendor collects HR information, including sensitive personally identifiable information, from NFC PPS and maintains it in their Employment Verification system for the purpose of providing relevant data to verifiers

²⁵ The claimant would still be a current employee since no significant personnel changes occur within NFC once an employee separates from DHS.



in support of credit and other business decisions regarding DHS employees. The information is also used to support state processing of Unemployment Compensation claims submitted by DHS employees. The information collected from NFC PPS includes Social Security number since it is typically used as the primary unique identifier both by verifiers and states. DHS also collects HR information directly from DHS employees and verifiers when registering them for accounts in its Employment Verification system. Additionally, the Employment Verification vendor collects relevant HR documentation requested by states when relevant to its processing of Unemployment Compensation claims submitted by DHS employees.

3.2 Does the project use technology to conduct electronic searches, queries, or analyses in an electronic database to discover or locate a predictive pattern or an anomaly? If so, state how DHS plans to use such results.

The Employment Verification vendor does not conduct electronic searches, queries, or analyses to locate a predictive pattern; however, the vendor does run an automated scan of each biweekly feed from NFC to identify patterns and anomalies suggestive of data inaccuracies. The reviews are programmed to identify duplicate data as well as data that is logically inconsistent (e.g., a change in Social Security number from the previous feed or number of hours worked not equating to reported wages). All suspected inaccuracies are flagged in an error report and associated to the individual's Social Security number so that an Employment Verification and Unemployment Compensation analyst can subsequently evaluate whether the data is indeed inaccurate. If it is, the Employment Verification and Unemployment Compensation vendor will inform DHS management, who will then further investigate and work with NFC to correct the information in NFC PPS and avoid similar errors in the future, as appropriate.

3.3 Are there other components with assigned roles and responsibilities within the system?

Each DHS Component designates several (generally 2-5) individuals who can access the Employment Verification and Unemployment Compensation system on behalf of DHS, as well as several (generally 2-5) individuals who serve as initial points of contact for HR documentation and other issues related to Unemployment Compensation claims processing. When a new employee attempts to register for an account as a DHS user, the Employment Verification and Unemployment Compensation vendor notifies the Employment Verification and Unemployment Compensation management team in DHS Headquarters, and that team then contacts the appropriate Component to validate the employee's need to know. DHS Headquarters maintains a roster of all DHS administrators and Unemployment Compensation points of contact to ensure they understand their roles and responsibilities and have completed necessary training, including annual privacy and IT security awareness training.



3.4 **Privacy Impact Analysis: Related to the Uses of Information**

Privacy Risk: There is a risk that inaccurate information in NFC PPS could lead to a faulty or unjust Employment Verification or Unemployment Compensation decision.

Mitigation: This risk is mitigated. NFC PPS data is automatically uploaded by the Employment Verification and Unemployment Compensation vendor with no human intervention, and all files are electronically scanned for patterns and anomalies suggestive of data inaccuracies as discussed in Section 3.2. Moreover, if data is inaccurate in NFC systems, it will often be identified prior to transmission to the Employment Verification and Unemployment Compensation vendor since it affects many other routine HR functions such as processing of compensation and benefits or regular personnel actions.

Privacy Risk: There is a risk that individuals could gain unauthorized access to information in the vendor's Employment Verification or Unemployment Compensation systems.

Mitigation: This risk is partially mitigated. The risk of access by malicious or unauthorized actors is inherent to all systems; however, the Employment Verification and Unemployment Compensation systems are required to comply with all relevant IT security and policy controls in DHS 4300A, the Sensitive System Handbook,²⁶ as a condition to maintaining their authority to operate in support of DHS. Specific controls include role-based access to Employment Verification and Unemployment Compensation systems and requiring system users to demonstrate a need-to-know the specific type of information is requested.

Privacy Risk: There is a risk that data in the Employment Verification and Unemployment Compensation vendor's possession may be used in a manner inconsistent with Employment Verification or Unemployment Compensation operations.

Mitigation: This risk is partially mitigated. Department personnel and contractors are required to sign acceptable use policies and complete annual records management and privacy training. Additionally, the vendor is required to comply with agency ethical standards and with the consumer protections contained in the Fair Credit Reporting Act. Failure to comply with these requirements will result in disciplinary action, up to and including removal or contract termination.

Section 4.0 Notice

4.1 **How does the project provide individuals notice prior to the collection of information? If notice is not provided, explain why**

²⁶ DHS 4300A Sensitive System Handbook is a series of information security policies, which are the official documents that create and publish Departmental security standards in accordance with DHS Management Directive 140-01, Information Technology System Security. See U.S. DEPARTMENT OF HOMELAND SECURITY, DHS 4300A SENSITIVE SYSTEMS HANDBOOK, available at <https://www.dhs.gov/publication/dhs-4300a-sensitive-systems-handbook>.



not.

The Employment Verification and Unemployment Compensation vendor systems landing pages for all users contains a link to a detailed privacy policy. The privacy policy includes a description of the type of information the vendor collects, how that information is used, and with whom it is shared. It also includes an email and physical mailing address for questions and comments about employee data protection or other privacy-related outreach. Other information the vendor collects in support of DHS's Employment Verification and Unemployment Compensation functions is not collected directly from individuals, but rather comes from NFC in biweekly data feeds or from states and territories processing Unemployment Compensation claims. States and territories follow their own laws and regulation regarding notice during submission of Unemployment Compensation claims. Notice is also provided by this Privacy Impact Assessment, as well as the publication of the system of records notices identified in Section 1.2. Additionally, information about DHS's Employment Verification and Unemployment Compensation functions is available to current DHS employees through the DHS intranet site.

4.2 What opportunities are available for individuals to consent to uses, decline to provide information, or opt out of the project?

DHS employees can configure their accounts in the Employment Verification system to indicate their refusal to allow any of their information to be shared with commercial verifiers by placing an employment data freeze on their file.²⁷ Additionally, a verifier can only access a DHS employee's information with a permissible purpose under the Fair Credit Reporting Act.

UC claims processing is initiated in response to an employee submitting Unemployment Compensation claim information with the unemployment insurance office in the state or territory where he or she resides. Because Unemployment Compensation is a voluntary public benefit, the employee may withdraw their Unemployment Compensation application or withdraw from receiving benefits at any time.

4.3 Privacy Impact Analysis: Related to Notice

Privacy Risk: There is a risk that DHS employees will not receive notice that they can opt out of DHS sharing their information with verifiers.

Mitigation: This risk is mitigated. New DHS employees are provided a brief presentation on Employment Verification and Unemployment Compensation services available to them during their onboarding. This includes information about how they can register for their Employment Verification system account, how they can use it to retrieve information about themselves that could be provided to verifiers, and how they can configure their accounts to opt out of having their

²⁷ Employees may not decline to have their information shared with government verifiers with a permissible purpose and proper jurisdictional authority.



information shared with commercial verifiers. Onboarding employees will also be provided with brochures and wallet-sized cards containing information about the Employment Verification service and the ability to enable notifications and alerts when commercial verifiers request their data. Additionally, information about the DHS Employment Verification and Unemployment Compensation Program generally, and about setting up and configuring employee accounts in the Employment Verification system specifically, will be posted on appropriate customer-facing pages of DHS intranet sites. The DHS Office of the Chief Information Officer (OCIO) will also send occasional emails to all DHS employees explaining the Employment Verification services available to them and how to register for an Employment Verification system account.

Section 5.0 Data Retention by the Project

5.1 Explain how long and for what reason the information is retained.

The following table summarizes the categories of information stored by the vendor and the controlling records schedules for each.

	Description	Disposition
Employee Management Administrative Records GRS 2.2, item 010 (DAA-GRS-2017-0007-0001)	Records on routine office program support, administration, and human resources operations.	Destroy when 3 years old, but longer retention is authorized if required for business use.
Individual Employee Records GRS 2.2, item 041 (DAA-GRS-2017-00070005)	Records of separated employees saved to the “temporary” folder in eOPF.	Destroy when superseded or obsolete, or upon separation or transfer of employee.
Notifications of Personnel Actions GRS 2.2, item 050 (DAA-GRS-	Copies of Standard Form 50, documenting all individuals personnel actions such as hiring, promotions, transfers, and separation.	Destroy when business use ceases.



2017-0007-0006)		
Payroll Records GRS 2.4, item 010 (DAA-GRS-2016-0015-0001)	Records used to calculate payroll, arrange paycheck deposit, and change previously issued paychecks.	Destroy 2 years after employee separation or retirement, but longer retention is authorized for business use.
Time and Attendance Records GRS 2.4, item 030 (DAA-GRS2016-0015-0003)	Sign-in/sign-out records, timecards, leave applications and approvals of all types (annual, sick, family medical, military service, jury duty, leave donations, etc.); overtime, compensatory, and credit time requests and approvals; premium pay authorizations; and other records documenting employees' presence at or absence from work.	Destroy when 3 years old but longer retention is authorized if required for business use.
GRS 2.5, item 010 Separation Program Management Records Not Specific to an Agency Separation Initiative (DAA-GRS-2014-0004-0001)	Records documenting the general work process to release career, temporary, and political-appointment employees from employment status.	Destroy when no longer required for business use.
GRS 2.5, item 011 Separation Program Management Records Specific to an Agency Separation Initiative	Records documenting the general work process to release career, temporary, and political-appointment employees from employment status.	Destroy 2 years after date of program closure, but longer retention is authorized if required for business use.



(DAA-GRS-2014-0004-0002)		
GRS 2.5, item 020 Individual Employee Separation Case Files (DAA-GRS-2014-0004-0003)	Records not included in the separating employee’s Official Personnel Folder, documenting individual employee’s transfer to another Federal agency or office or voluntary, involuntary, disability, early retirement, retirement, or death separation from career, temporary, and political appointment service; and legal and financial obligations of government to employee and employee to government.	Destroy 1 year after date of separation of transfer, but longer retention is authorized if required for business use.

The Fair Credit Reporting Act mandates that Employment Verification reports be retained for at least five (5) years for dispute resolution purposes. The Employment Verification and Unemployment Compensation vendor retains these reports for an additional two (2) years beyond this five-year minimum to address potential audits or litigation. Retention for Unemployment Compensation records are established by the various states and territories that manage unemployment insurance programs, with the longest retention period set at eight (8) years. The Employment Verification and Unemployment Compensation vendor retains records for an additional six (6) months beyond this longest eight-year retention to address potential audits or litigation.

5.2 Privacy Impact Analysis: Related to Retention

Privacy Risk: There is a risk the Employment Verification and Unemployment Compensation vendor will retain data on DHS employees longer than is necessary to accomplish a legitimate purpose, or inconsistently with the records retention schedule.

Mitigation: This risk is mitigated. The Employment Verification and Unemployment Compensation vendor has configured its systems so that DHS employee records are automatically purged after seven (7) years in the case of Employment Verification records, and after eight (8) years and six (6) months in the case of Unemployment Compensation records.

Section 6.0 Information Sharing

6.1 Is information shared outside of DHS as part of the normal



agency operations? If so, identify the organization(s) and how the information is accessed and how it is to be used.

The Employment Verification and Unemployment Compensation vendor routinely shares information with credentialed verifiers as part of Employment Verification operations. This sharing takes the form of verification of employment only, verification of both employment and income, and Social Services Verifications reports that are also accessible to employees on demand. The Employment Verification and Unemployment Compensation vendor also shares information with states and territories at their request when they receive an Unemployment Compensation claim submission from a current or former DHS employee. This information sharing consists of standard responses to state data requests, fulfilled in the form of open text fields and dropdown menus in the Unemployment Insurance Interstate Connection Network (as described in Section 2.1). It also consists of HR documentation collected in special cases at the state's request and delivered by regular U.S. mail. Any other sharing outside of DHS is limited to rare circumstances described in the routine use sections of the applicable system of records listed in Section 1.2 above.

6.2 Describe how the external sharing noted in 6.1 is compatible with the SORN noted in 1.2.

OPM/GOVT-1 routine use D allows DHS to disclose general personnel information to a national, state, county, municipal, or other publicly recognized income security administration agency (e.g., state unemployment compensation agencies), when necessary to adjudicate a claim under the retirement, insurance, unemployment, or health benefits program. This is compatible with the Employment Verification and Unemployment Compensation vendor sharing data with states in support of their processing of Unemployment Compensation claims submitted by DHS employees.

OPM/GOVT-1 routine use DD allows DHS to disclose general personnel information to prospective non-federal employers the following information about a specifically identified current or former federal employee: tenure of employment, civil service status, length of service in the agency of the government; and when separated, the date and nature of action as shown on the SF-50. This is compatible with the Employment Verification and Unemployment Compensation vendor sharing data with commercial verifiers requesting reports in support of hiring decisions.

DHS/ALL-019 routine use Q allows DHS to disclose payroll, personnel, and time and attendance records to state offices of unemployment compensation. This is compatible with the Employment Verification and Unemployment Compensation vendor sharing data with states in support of their processing of Unemployment Compensation claims submitted by DHS employees.

DHS/ALL-019 explicitly states after its list of routine uses that, pursuant to 5 U.S.C. §



552(a)(b)(12), disclosures may be made from the system to consumer reporting agencies as defined in the Fair Credit Reporting Act. This is compatible with DHS sharing employment and income data of DHS employees with the Employment Verification and Unemployment Compensation vendor who serves in the capacity of a consumer reporting agency when verifying employment and income to commercial and government verifiers with a permissible purpose.

6.3 Does the project place limitations on re-dissemination?

The Employment Verification and Unemployment Compensation vendor has an interconnection security agreement (ISA) in place with NFC for the employee data it receives from NFC PPS. The ISA expressly limits re-dissemination outside of the scope of the Employment Verification and Unemployment Compensation contract with DHS. The ISA also expressly prohibits any activity that compromises, or has the potential to compromise, the confidentiality of client information. Moreover, the interconnection security agreement explicitly prohibits users from sending, uploading, removing on portable media, or otherwise transferring to a non-Employment Verification or Unemployment Compensation vendor system any Employment Verification or Unemployment Compensation information or data without prior express consent that includes the exact nature of the data, the receiver of the data, and the method of access control.²⁸

Additionally, the contract between the Employment Verification and Unemployment Compensation vendor and DHS places limitations on re-dissemination. For example, section 4.2(d)(2) of the contract states “the contractor shall not use or redistribute any sensitive information processed, stored, and/or transmitted by the contractor except as specified by the contract.” Under the contract, vendor employees are also required to execute DHS Form 11000-6, Department of Homeland Security Non-Disclosure Agreement (NDA) as a condition of access to any sensitive personally identifiable information, and the vendor is required to maintain signed copies of the signed Non-Disclosure Agreements for all employees as a record of compliance. Furthermore, the contract incorporates by reference the DHS Handbook for Safeguarding Sensitive Personally Identifiable Information,²⁹ as well as DHS 4300A, Sensitive Systems Handbook, Section 3.14.8 Use Limitation and External Sharing.

6.4 Describe how the project maintains a record of any disclosures outside of the Department.

The Employment Verification and Unemployment Compensation vendor systems maintain audit logs of all information transmissions, including all disclosures from the Employment

²⁸ This language is also reflected in the Employment Verification and Unemployment Compensation vendor’s internal Acceptable Use Policy.

²⁹ See Handbook for Safeguarding Sensitive Personally Identifiable Information (December 2017), *available at* <https://www.dhs.gov/publication/handbook-safeguarding-sensitive-personally-identifiable-information>.

Verification and Unemployment Compensation vendor to non-DHS entities. The logs track who transmitted the information, what information was transmitted, the date and time of transmission, and where it was sent. This information is maintained in the Employment Verification and Unemployment Compensation vendor's audit logs for a minimum of one year.

6.5 Privacy Impact Analysis: Related to Information Sharing

Privacy Risk: There is a risk that individuals authorized to directly access wage and employment information in the Employment Verification system will conduct unauthorized activities such as extracting and sharing information with unauthorized recipients.

Mitigation: This risk is partially mitigated. Although there are no physical or technical barriers preventing system administrators from extracting information from Employment Verification and Unemployment Compensation vendor systems and sharing it with unauthorized recipients, they are required to sign an acceptable use policy prohibiting such practices as a condition of employment. Additionally, all user accounts require approval from the DHS system owner and DHS Information System Security Officer. The Employment Verification and Unemployment Compensation system also contains audit history logs detailing who accessed the system and when, as well as what information they accessed and shared. The DHS Office of the Chief Information Officer is planning to review scans and logs from the vendor on a periodic basis. Furthermore, all Employment Verification and Unemployment Compensation vendor employees with access to DHS information are required to sign the DHS Form 11000-6 and to take mandatory DHS privacy and IT security training that explains any improper sharing could result in removal from the contract and possible legal action.

Section 7.0 Redress

7.1 What are the procedures that allow individuals to access their information?

Employees (or former employees³⁰) may access their information by creating a user account in the Employment Verification and Unemployment Compensation vendor system, which will then enable them to download on demand the same verification of employment only, verification of both employment and income, and Social Services Verifications reports credentialed verifiers can request about them. Additionally, employees may access personal data about themselves maintained by NFC via MyEPP. Employee records collected, maintained, and disseminated by DHS and its Employment Verification and Unemployment Compensation vendor are also covered by the Privacy Act, and employees may file a Privacy Act or Freedom of

³⁰ The user accounts that employees can create with Equifax do not depend on their employment with DHS or anywhere else. Anyone can create a user account with any of the credit monitoring agencies to review their credit information and what credentialed verifiers can see about them.



Information Act request with DHS or NFC to access their personnel records.

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

Employees who identify incorrect information about themselves within their Employment Data Report are instructed on the Employment Verification and Unemployment Compensation vendor's website to contact the Employment Verification and Unemployment Compensation vendor support team to initiate a dispute. Employees can submit disputes to the Employment Verification and Unemployment Compensation vendor through its website, postal mail, fax, telephone, and email. The support team will then notify the Employment Verification and Unemployment Compensation management team in DHS Headquarters as well as a designated point of contact within the employee's Component, as appropriate. These management personnel will investigate other HR records to validate that the information is indeed inaccurate. If it is, DHS Headquarters will reach back to the Employment Verification and Unemployment Compensation vendor to have the information corrected within its systems and will also work with NFC to correct the information in NFC PPS to ensure similar inaccuracies do not occur in the future, as appropriate.

If an employee knows of any inaccurate or erroneous information about himself or herself in any other HR system, regardless of whether it is associated with Employment Verification and Unemployment Compensation, the employee may contact the appropriate HR specialist within his or her human resources servicing unit. This individual will then liaise with the appropriate IT personnel at the source system agency or database to correct the information. The employee may also submit an HR ticket through FedHR Navigator³¹ or through other Component-specific human resources IT ticketing mechanisms to request correction of inaccurate or erroneous information in any DHS record or system.

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

The Employment Verification system site has a support team email listed at the bottom of its landing page. Additionally, each DHS organization has one or more dedicated HR specialists to assist with HR needs. The names and titles of these individuals are common knowledge throughout organizations and are reflected on organization charts. Employees may also reach out to the DHS Office of the Chief Human Capital Officer (OCHCO) or any of the Component human

³¹ FedHR Navigator is a commercial-of-the-shelf system that automates federal HR functions and assists the strategic management of human capital within the federal workforce. It is used by certain DHS Components and certain other agencies throughout the Federal Government and consists of a suite of web-based software tools accessible by employee and HR personnel. More information about FedHR Navigator may be found on the FedHR Navigator website, available at <https://www.econsys.com/fedhr-navigator/>.



capital offices using the general HR phone numbers and email addresses posted on the DHS employee intranet site. Additionally, they may submit an HR service ticket through FedHR Navigator to correct inaccurate information, or they may correct some of their personal information themselves using MyEPP. Links to FedHR Navigator and MyEPP are prominently displayed on the DHS employee intranet homepage.

7.4 Privacy Impact Analysis: Related to Redress

Privacy Risk: There is a privacy risk that employees will not be able to access, correct, or amend their personnel records in the Employment Verification and Unemployment Compensation vendor systems or the NFC PPS source system from which it obtains its employee data.

Mitigation: This risk is mitigated. Contact information for the Employment Verification and Unemployment Compensation vendor's support team is prominently displayed in the Employment Verification system. Regarding the NFC source system from which the vendor obtains its employee data, employees have HR representatives assigned to them who can assist with this and other types of HR matters. Employees also routinely use MyEPP to update and correct their personnel data. Additionally, all government personnel records are covered by the Privacy Act, and fall under the general personnel records system of records notices managed and maintained by DHS and NFC. There are Privacy Act notices on all NFC and DHS IT systems at the points of collection that alert employees that their records are afforded Privacy Act protections.

Section 8.0 Auditing and Accountability

8.1 How does the project ensure that the information is used in accordance with stated practices in this PIA?

Privacy controls described in this Privacy Impact Assessment are written into the Employment Verification and Unemployment Compensation vendor's contract with DHS. These include limits on the use of Social Security number, role-based access to sensitive information, Non-Disclosure Agreements for all personnel working on the contract, and a requirement to comply with major DHS privacy-related policies such as the DHS Handbook for Safeguarding Sensitive Personally Identifiable Information, the DHS Privacy Incident Handling Guide,³² and the DHS 4300A, Sensitive Systems Handbook and Attachments. The Employment Verification and Unemployment Compensation vendor is also required to continuously comply with a comprehensive set of privacy controls contained in its DHS-approved System Security Plan as a condition to maintaining its Authority to Operate. These controls cover a wide range of issues central to privacy program management, including monitoring and auditing, awareness and training, incident reporting and response, system design and development, data quality and

³² See DHS Privacy Incident Handling Guide (December 2017), available at <https://www.dhs.gov/publication/privacy-incident-handling-guidance-0>.



integrity, data minimization, data retention and disposal, consent, individual access, redress, authority to collect, purpose specification, internal program governance, risk assessment, and notice to system users and to the public.

8.2 Describe what privacy training is provided to users either generally or specifically relevant to the project.

The Employment Verification and Unemployment Compensation vendor requires all its employees to complete a general training course that covers privacy and IT security awareness on an annual basis as a condition of employment. DHS also requires all employees who work on its Employment Verification and Unemployment Compensation contract to complete DHS-provided privacy and IT security awareness training within 30 days of starting work on the contract and annually thereafter. The Employment Verification and Unemployment Compensation vendor is required to maintain the DHS training completion certificates of its employees and to provide copies to their designated DHS Contracting Officer Representative (COR) as a record of compliance.

8.3 What procedures are in place to determine which users may access the information and how does the project determine who has access?

The Acceptable Use Policy that all Employment Verification and Unemployment Compensation vendor employees must annually sign requires users to take all necessary steps to prevent unauthorized access to confidential information, to refrain from re-disseminating Employment Verification and Unemployment Compensation information without prior express consent, to secure confidential information via encryption and by other means, to complete confidentiality and security awareness training, and to promptly report the theft, loss, or compromise of any confidential information. All of these practices are also included in the interconnection security agreement described in Section 6.3. Furthermore, all Employment Verification and Unemployment Compensation vendor employees who are provided access to DHS employee information must complete DHS's normal pre-onboarding process. This involves suitability checks to determine fitness of character (e.g., fingerprint collection and analysis, credit checks, drug test) and their formal attestation to abide by all DHS policies and procedures regarding privacy and the protection of personally identifiable information.

8.4 How does the project review and approve information sharing agreements, MOUs, new uses of the information, new access to the system by organizations within DHS and outside?

All interconnection security agreements, memoranda of understanding, new uses of information, and new access to Employment Verification and Unemployment Compensation



systems are reviewed by the DHS Headquarters Employment Verification and Unemployment Compensation Operations Team, with consultation from Components as appropriate. They are also reviewed and approved by the DHS Employment Verification and Unemployment Compensation system owner and by the DHS Employment Verification Contracting Officer Representative. Additionally, they are documented in the Employment Verification Unemployment and Compensation System Security Plan and thus subject to review and approval by DHS's Office of the Chief Information Security Officer. Certain documents reflecting new uses of information or new access by organizations may also be subject to review by the DHS Privacy Office, DHS Office of the General Counsel, and DHS Office of the Chief Procurement Officer, depending on how substantially they impact significant terms in the Employment Verification and Unemployment Compensation vendor's contract.

Contact Official

Courtney McGowan
Acting Director, Vendor Management and Customer Experience
Human Capital Business Solutions, Office of the Chief Human Capital Officer
courtney.mcgowan@hq.dhs.gov

Responsible Official

Neil Singh
Executive Director
Human Capital Business Solutions, Office of the Chief Human Capital Officer
neil.singh@hq.dhs.gov

Approval Signature

Original, signed copy on file with the DHS Privacy Office

Lynn Parker Dupree
Chief Privacy Officer
U.S. Department of Homeland Security
(202) 343-1717