PRIVACY IMPACT ASSESSMENT

Effective Date: April 13 2026

Bureau of Labor Statistics (BLS)

National Longitudinal Survey of Youth, 2027 (NLSY27)

NLSY27 System

☒Concurrence of Senior Agency Official for Privacy

☐Non-concurrence of Senior Agency Official for Privacy

BRAYE CLOUD Digitally signed by BRAYE CLOUD
Date: 2026.04.13 11:56:15 -04'00'

Braye Cloud, Senior Agency Official for Privacy (SAOP)
Deputy Assistant Secretary for Operations
Office of the Assistant Secretary for Administration & Management

OVERVIEW & GENERAL INFORMATION

As required by the E-Government Act of 2002 (as amended) and OMB Memorandum M-03-22, National Longitudinal Survey program has developed this Privacy Impact Assessment to describe:

1. The information to be collected with a particular focus on personally identifiable information (PII);
2. Why the information is being collected including the legal authority for the information collection;
3. The intended use of the information;
4. With whom the information will be shared (such as internal uses with other DOL component agencies or another federal agency);
5. What notice is provided to individuals, what opportunities are given to individuals to consent to particular uses of the information, how individuals can grant consent, and what opportunities individuals have to decline to provide information;
6. How the information will be secured with administrative and technological security controls;
7. Whether a *system of records* is being created under the Privacy Act, 5 U.S.C. 552a; and
8. The analysis of privacy risk associated with the collection, use, storage, and dissemination of information and practices that have an impact on privacy.

Name of System (and Acronym, if applicable)

National Longitudinal Survey 27 System (NLSY27)

Location of the System

The NLSY27 system is composed of two separate entities, (BLS and RTI International (RTI)), that each have their own operating environments, configuration settings, security documentation, and physical locations. The BLS entity resides at the BLS Headquarters. It consists of electronic systems; it is accessed primarily onsite but may be accessed remotely by authorized users. The RTI entity includes physical locations maintained by RTI. Records at RTI are securely controlled in compliance with FIPS Moderate requirements, whether electronic (encrypted in our private firewalled NLSY27 System) or paper-based (in secure, accessed controlled, locked facilities and cabinets when not in use) and only accessible to designated individuals.

Brief Description of the System

The NLSY27 is a new cohort of the National Longitudinal Surveys (NLS) Program of the Bureau of Labor Statistics (BLS) whose first round of interviewing is planned to begin in the Fall of 2027 for approximately 17,000 youth and their parents/caregivers. The sample will be identified through short screener surveys to be completed by the youth's parents or caregivers, which will begin collection in August 2027. Prior to that start, BLS plans to conduct a Pretest in early 2026, in which approximately 800 youth and their parents/caregivers will be interviewed. In order to allow for the Pretest to occur on schedule, BLS intends to receive an Authority to Operate (ATO) for this system

in early 2026 under the National Institute of Standards and Technology (NIST) Special Publication 800-53 for Federal Information Processing Standards Moderate classification as assessed by an accredited Third-Party Assessment Organization (3PAO). The NLSY27 System will principally be housed and maintained through BLS's contractor, RTI International (RTI) in a private, encrypted, and secure computing center environment created by RTI for the NLSY27 Pretest and Round 1 collections. It will include an electronic case management system that: screens households; determines parental/caregiver and youth eligibility; performs consent and assent of eligible participants; administers parental/caregivers and youth Round 1 Surveys; monitors progress and production goals versus actuals; and securely processes data per BLS requirements.

Purpose of the System:

☐ Program administration	☐ Employee or customer satisfaction surveys
☐ Computer Matching Program	
☐ Administering human resources programs for DOL or federal government personnel	☐ Improve Federal services online
☐ Litigation	☐ Promote information sharing initiatives
☐ Criminal law enforcement activities	☐ Civil law enforcement activities
☒ Other: To administer a survey	

This System is operated by:

☐ Component agency

☒ Contractor

For a system operated by a contractor, the contract or other acquisition-related documents includes privacy requirements:

☒ Yes
☐ No

This PIA is being conducted for:

☒ A new information system or project that collects, maintains, or disseminates information in identifiable form.

☒ A new collection of information subject to the Paperwork Reduction Act because it is for 10 or more persons (excluding agencies, instrumentalities, or employees of the federal government in the scope of their employment).

☐ A change to the PII Confidentiality Impact Level (NIST SP 800-122) or System Security Categorization (NIST SP 800-60).

☐ An existing system subject to a periodic review at the 3-year mark.

☐ An existing system with significant changes that create new privacy risks.

The following are the significant changes that create new privacy risks:

☐ Changed information collection authorities.

☐ Changed business processes.

☐ Conversion of paper-based records to electronic systems.

☐ Anonymous to Non-Anonymous. This is when functions applied to an existing system change anonymous information into information in identifiable form.

☐ Significant System Management Changes. This is when new uses of an existing IT system, including application of new technologies, significantly change how information in identifiable form is managed in the system.

☐ Significant Merging. This is when agencies adopt or alter business processes so that government databases holding information in identifiable form are merged, centralized, matched with other databases or otherwise significantly manipulated.

☐ New Public Access. This is when user-authenticating technology (e.g., password, digital certificate, biometric) is newly applied to an electronic information system accessed by members of the public.

☐ Commercial Sources. This is when agencies systematically incorporate into existing information systems databases of information in identifiable form purchased or obtained from commercial or public sources.

☐ New Interagency Uses. This is when agencies work together on shared functions involving significant new uses or exchanges of information in identifiable form.

☐ Internal Flow or Collection. This is when alteration of a business process results in significant new uses or disclosures of information or incorporation into the system of additional items of information in identifiable form.

☐ Alteration in Character of Data. This is when new information in identifiable form added to a collection raises the risks to personal privacy (for example, the addition of health or financial information).

☐ Other.

The class(es) of users who will have access to the system are:

☐ General Public
☒ Contractors
☒ Government Employees
☐ Other

1. INFORMATION IN THE SYSTEM

BLS collects certain types of information from certain sources using particular methods to collect the information, as identified below.

1.1. The information that is collected, used, maintained, or disseminated in connection with the system is:

☒ Name/Former Name	☒ Date of Birth	☐ Maiden Name	☒ Place of Birth	☐ Citizenship
☒ Social Security number (including in truncated form)	☐ Driver's License	☐ Financial Account	☐ Taxpayer ID	☐ Passport Number
☒ Sex	☒ Telephone Number	☒ Criminal Record	☒ Education	☒ Age
☐ Financial Transaction	☐ Employer ID	☐ Alien Registration Number	☐ Vehicle Identifier	☐ Employee ID
☐ Credit Card	☐ Medical Record	☐ File/Case ID	☒ Financial Information	☒ Religion
☐ Alias	☒ Home Address	☒ Military Service	☒ Mother's Maiden Name	☒ Medical Information
☒ Email Address	☒ Marital Status	☒ Race/Ethnicity	☒ Occupation	☐ Work Email Address
☐ Job Title	☒ Salary	☐ Business Associates	☐ Work Telephone Number	☐ Proprietary or Business Information
☐ Employment Performance Ratings	☐ Work Address	☒ Work History	☐ Procurement or contracting records	☐ Other Performance Information
☐ Fingerprints	☐ Scars, Marks, Tattoos	☐ Signatures	☐ Photographs	☐ Palm Prints
☐ Hair Color	☐ Vascular Scans	☒ Weight	☒ Voice/Audio Recording	☐ Eye Color
☐ DNA Sample or Profile	☐ Dental Profile	☐ Video Recording	☒ Height	☐ Retina/Iris Scans

☐ User ID	☒ IP Address	☒ Other PII. Control Number, Family Structure, Substance Use history, and Government Program Participation

1.2. The information is collected using the following methods:

☒ Website-based forms
☒ Paper forms
☒ Electronic forms
☒ Verbal collection
☐ No form - the information collected does not require a specific form

1.3. The source of the information is:

Directly from the Individual about Whom the Information Pertains		
☒ In Person	☒ Hard Copy: Mail/Fax	☒ Web-based (uploading through an app or website)
☒ Telephone	☒ Email	☐ Legal or other representative.
☐ Other		

Government Sources		
☐ Within the Component Agency	☐ Other DOL component agencies	☐ Other Federal Agencies
☐ State, Local, Tribal	☐ Foreign	☐ Other

Non-government Sources		
☐ Public Organizations	☐ Private Sector	☐ Commercial Data Brokers
☐ Third Party Website or Application	☐ Third Party Website or Application	☐ Other

1.4. Social Security numbers (SSN) are collected:

The Privacy Act of 1974 requires that when DOL requests that an individual provide a Social Security number, DOL must indicate whether that disclosure is mandatory or voluntary and by what statutory or other authority the number is being requested including what uses will be made of it.

Additionally, OMB Circular A-130 to the Heads of Executive Departments and Agencies regarding *Managing Information as a Strategic Resource* includes a requirement that DOL take steps to eliminate unnecessary collection, maintenance, and use of Social Security numbers, and explore alternatives to the use of Social Security numbers as a personal identifier.

Finally, DOL policies permit component agency programs to collect, use, maintain, and disseminate SSNs only when required by law (e.g., statute, regulation, or upon approval of the SAOP or SAOP designee).

Will SSNs be collected for this system, whether directly or indirectly from the individual to whom the SSN applies?

☐ No
☒ Yes

1.4.1. If yes, the specific authority relied upon to collect SSNs?

Since the collection of SSNs is not expressly permitted by a statute, a request to collect SSNs was approved by DOL's Senior Agency Official for Privacy (SAOP) in February 2025.

1.4.2. The purpose for the collection of SSNs and how the SSN will be used is as follows:

SSNs will be collected to facilitate future locating efforts for maintaining long-term contact with survey participants, adhering to strict protocols for use only during the extended administration of the NLSY27 survey.

1.4.3. The following alternatives were considered in lieu of the collection of SSNs:

Alternatives considered included forgoing SSNs used during locating efforts and increasing the contact of relatives and associates of survey participants.

1.4.4. The alternatives were not selected because:

These alternatives were not selected because they would be expected to be less effective, degrading the value of the survey. In addition, they would increase the burden experienced by family and associates of sample members.

1.5. The information collected is subject to the Paperwork Reduction Act:

☒ Yes, some or all of the information is covered by the Paperwork Reduction Act.
- ☒ The information expected to be collected does not yet have an OMB control number but will be submitted for PRA approval.
- ☐ The information collected is part of an existing collection and the OMB control number for the collection is.

☐ No, the information collected is not subject to the Paperwork Reduction Act.

2. WHY THE INFORMATION IS BEING COLLECTED

2.1. Why is the information being collected?

The NLSY27 is designed to meet the purposes described by Congress: to "fill critical gaps in data about the new generation of young workers" that the NLSY79 and NLSY97 surveys would miss and to provide "an understanding of how this new generation's actions and choices are affected by our changing economy." Since the last NLS cohort was initiated in 1997, many influences such as technological advances, changes in social norms, and the rise of new modes of communication have altered schooling and the structure of the labor market. Through consultation with a wide range of stakeholders, BLS is giving extensive consideration to how the new youth cohort can best meet these purposes, as well as serving the data needs of the Department of Labor and other agencies. Several qualities in the data are important, including:

- nationally representative samples with sufficient demographic variation to enable cross-group comparisons;
- adequate sample sizes within birth cohorts for studying labor market outcomes;
- data spanning multiple life domains;
- measures of a broad range of individual and family characteristics that affect and are affected by labor market outcomes;
- inclusion of cognitive assessments in addition to survey responses; and
- inclusion of measures of factors that are unique to today's youth as well as measures that facilitate comparisons to earlier NLSY cohorts.

2.2. The following are the specific legal authorities and/or agreements that permit the collection, use, maintenance, and/or dissemination of information (including any PII) by the system:

This study is authorized under Title 29, Section 2 of the United States Code.

3. INTENDED USE OF THE INFORMATION

3.1. The information collected by the system is used in the following ways:

PII is used to: 1) determine eligibility at the household and participant levels during screening; 2) frame later questions in the surveys to assist with collecting accurate information; 3) derive and create variables so BLS analysts and economists can address NLSY27 aims and objectives; 4) enable future data collections (e.g., providing information to help BLS locate and contact respondents for additional survey rounds); and 5) enable BLS-authorized researchers to link the collected data to other datasets to produce valuable statistics (note that such linkages will only be performed in a restricted data environment and that only aggregate statistics that have been cleared by BLS confidentiality review will be released).

3.2. The system aggregates or analyzes information to create new information:

☐ Yes
☒ No

4. INFORMATION SHARING AND ACCESS

4.1. Will BLS share data internally or externally?

☒ Yes, the PII in the system will be shared.
☐ No, The PII in the system will not be shared.

Internal Sharing:

Component Agency	Information Shared	Purpose

External Sharing:

Organization	Information Shared	Purpose	MOU or other Agreement
RTI	RTI staff will have access to the collected PII on the least privileged basis.	To develop and administer the survey	Work is being performed under contract 1605-C5-23-F-00035.
Mass Texting Service	An external contractor providing mass texting will have access to respondent phone numbers.	Distribution of mass texts to promote survey participation	Customer agreement with RTI.

4.2. Does BLS place a limitation on re-dissemination of PII shared with internal or external organizations?

Internal Sharing

☐ Yes, another DOL component agency is required to verify with the component agency operating the system before re-dissemination of PII.

☐ No, another DOL component agency is not required to verify with the component agency operating the system before re-dissemination of PII.

☒ Not applicable, the component agency does not share PII with other DOL component agencies.

External Sharing

☒ Yes, the external agency or entity is required to verify with the DOL component agency before re-dissemination of PII.
RTI may not share the PII with any other entity besides BLS; sharing PII with BLS is done only as specifically requested and authorized by BLS. The mass texting service may not use the respondent's phone numbers for any other reason except to send the texts that have been specifically authorized.

☐ No, the external agency or entity is not required to verify with the DOL component agency before re-dissemination of PII.

☐ Not applicable, the component agency does not share PII with external agencies or entities.

4.3. Indicate whether the system connects with or receives information from any other systems authorized to process PII.

☐ Yes, this system connects with or receives information from another system(s) authorized to process PII.

If the answer to 4.3 is yes, provide the name of the system and describe the technical controls which prevent improper accessing of the PII while in transit.

☒ No, this system does not connect with or receive information from another system(s) authorized to process PII and/or BII.

5. NOTICE, CONSENT, AND OPPORTUNITY TO DECLINE TO PROVIDE INFORMATION

5.1. Indicate whether individuals will be notified if their PII is collected, maintained, or disseminated by the system.

☒ Notice is provided pursuant to a system of records notice published in the Federal Register and discussed in Section 7.

☒ Notice is provided by a Privacy Act Statement and/or a Privacy Notice. The Privacy Act Statement and/or Privacy Notice can be found on the following forms or information collection instruments: Parent/guardian permission form and Youth assent form (which is required to be completed for the collection of the youth instrument); Parent/caregiver consent form (which is required to be completed for collection of the parent/caregiver instrument)

☐ Notice is provided by other means.

☐ Notice is provided by means of this Privacy Impact Assessment.

5.2. Do individuals have an opportunity to decline to provide PII?

☐ Yes, individuals have an opportunity to decline to provide PII.

☒ No, individuals do not have an opportunity to decline to provide PII.
No, individuals participating in the survey cannot decline to provide PII. PII is required to conduct the survey and assist in participant locating efforts.

5.3. Do individuals have an opportunity to consent to particular uses of their PII?

☒ Yes, individuals have an opportunity to consent to particular uses of their PII.
Respondents sign a consent form prior to the collection of any PII. The form states there are two exceptions to our promise of confidentiality: 1)if the respondent tells the interviewer that they plan to seriously harm themselves or others, that information will be shared with a parent (guardian) and RTI will report that information to BLS NLSY27 staff, and 2) if the interviewer suspects abuse or neglect of a child or adult, RTI and BLS will follow laws for reporting child and adult abuse.

☐ No, individuals do not have an opportunity to consent to particular uses of their PII.

5.4. Do individuals have an opportunity to review or update PII pertaining to them?

☒ Yes, individuals have an opportunity to review or update PII pertaining to them.
Participants may contact RTI or BLS to amend information.

☐ No, individuals do not have an opportunity to review or update PII pertaining to them.

6. HOW INFORMATION IS SECURED

As required by the E-Government Act of 2002 and OMB Memorandum M-03-22, DOL imposes certain administrative and technological controls on each system that contains PII. Below, DOL describes whether it has conducted a risk assessment, the security controls to put in place to protect against that risk, and how those controls are implemented. DOL also describes how it continuously monitors the system to ensure that the controls continue to work properly, safeguarding the information. Individuals who have questions regarding the information below may reach out to DOL's Privacy Program at privacy@dol.gov.

6.1. Administrative controls for the system:

☒ PII is kept in a secured physical location.
Yes, all SSNs are in a secured physical location and encrypted per NIST SP 800-53 requirements and FIPS 140 standards.

☒ All users signed a confidentiality agreement or non-disclosure agreement.
Identify the agreement(s) signed.

☒ All users are subject to a Code of Conduct that includes the requirement for confidentiality.
BLS Rules of Behavior (https://labornet.dol.gov/itc/it/IT-Security/BLS-Rules-of-Behavior.htm) and DOL Rules of Conduct Concerning PII (https://labornet.dol.gov/itc/it/IT-Security/Rules-of-Conduct-Failure-to-Safeguard-PII.htm)

☒ DOL Personnel (employees, contractors, interns, volunteers) receive **annual** training on privacy and confidentiality policies and practices.
Privacy, confidentiality, and security are required annual training. Completion of these required trainings are tracked, retained, and made available to BLS.

☒ DOL Personnel receive **role-based** training on privacy and confidentiality policies and practices.
The NLS Information System Security Officer and NLS System Owner frequently take trainings, review materials, and consult with BLS's Department of Management Systems and BLS's Division of Network and Information Assurance to continuously improve their abilities to perform their roles. RTI staff participate in annual or periodic training programs to maintain compliance with all regulatory commitments and contractual obligations.

☒ DOL Personnel (employees, contractors, interns, volunteers) receive **system-specific** training on privacy and confidentiality policies and practices.

☒ Access to the PII is restricted to authorized personnel only.
PII in the NLSY27 system will be accessed on a role-based, need-to-know basis, following the principle of least privilege. Only designated individuals will have access to PII.

☐ Appropriate NIST SP 800-53 Revision 4 security controls for protecting PII are imposed.
  ☐ A security assessment report has been prepared for the information system to identify all privacy risks for continuous monitoring.

☒ Appropriate NIST SP 800-53 Revision 5 security controls for protecting PII are imposed.
  ☒ A security assessment report has been prepared for the information system to identify all privacy risks for continuous monitoring.
  The SAR was performed from September, November, December 2025, and January 2026.

☐ There is one or more Plan of Action and Milestones (POA&M) associated with this system.

☒ Contractors that have access to the system are subject to information security provisions in their contracts required by DOL policy.
Contract 1605-C5-23-F-00035, Task 2: Security
☒ Contracts with customers establish DOL ownership rights over data including PII.
BLS Letters of Agreement to be completed with authorized data users as approved by BLS
☐ Other

6.2. Technological controls for the system:

☒ Access to the PII is being monitored, tracked, or recorded:
Access to PII is tightly controlled. It is monitored, tracked, and reported, using the system's security information and event management (SIEM) tools, and administrative controls like logging and auditing.
☒ User Log In Credentials
Two-factor authentication is required for all end users (non-privileged) network access. End users utilitze a username and token (Vasco Identikey and PIN, and a separate domain level username and password) to access the network. These these authentication mechanisms are required to access internal resources via SFTP or Citrix.
☒ Virtual Private Network (VPN)
RTI utilizes a VPN appliance solution for access from the Internet to specific RTI networks.
☐ Biometrics
☒ Encryption of Data at Rest
All data residing on the system storage and backup storage in both the RTI primary and secondary data centers are encrypted at rest.
☒ Firewall
The perimeter and data center firewalls protect all network communication in and out of the Moderate network. The firewalls control traffic between the Moderate DMZ Networks and Data Center Network as well as to/from the Internet. Network engineers implement firewall rules to control traffic flow between interfaces. These rules are configured to monitor network traffic for malicious behavior and other specific attack signatures. Users within the Moderate Network are unable to access the Internet directly, except for websites approved for business purposes.
☒ Role-based Access Controls
The NLSY27 system is accessed on a role-based, need-to-know basis, following the principle of least privilege.
☒ Encryption of Data in Transit
The system encrypts data in transit.
☒ Use Only for Privileged (Elevated Roles)
Access to the separate PII database is tightly controlled. Only authorized BLS employees and RTI contracted staff can have access, and such access is narrowly defined to meet the role played by each individual. Access determination follows the rules described in NIST SP 800-53 and is fully audited. Training is conducted annually.
☐ Other

6.3. Retention of Information

Information in the system is covered by an approved records retention schedule and monitored for compliance.

☒ Yes.
Bureau of Labor Statistics (BLS) Statistical Programs Bucket Records Schedule N1-257-11-1
☐ No.
☐ A records retention schedule is in development.

If there is an approved record retention schedule, is retention monitored for compliance to the schedule?

☒ Yes, retention is monitored for compliance to the schedule.
☐ No, retention is not monitored for compliance to the schedule.
☐ No, there is not an approved record retention schedule.

When information is no longer needed, it is disposed of by:

☒ Shredding or other physical destruction
☒ Overwriting
☒ Physical destruction of hardware, such as degaussing
☒ Deleting
☐ Other

7. SYSTEM OF RECORDS NOTICE (SORN)

The Privacy Act of 1974 (Privacy Act) requires DOL to permit individuals to gain access to their records (including obtaining copies and requesting amendments to the records) and any information pertaining to the requesting individual which is contained in a "system of records" (a specifically defined term under the Privacy Act). Although many DOL Information Systems may contain PII, they are not all required to have a SORN. For purposes of the Privacy Act, a system of records that requires a SORN refers to any group of any records under the control of DOL (including through a contractor) from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual. Some systems of records under DOL's control may be exempt from some of the Privacy Act rights provided to individuals. DOL is identifying all of the SORNs applicable to this system so that individuals may review the SORNs for more detailed additional information.

7.1. This system is covered by one or more existing SORNs.

SORN has not yet been established; it is in development.

7.2. This system:

☐ Does not require an additional SORN beyond those identified above.

☐ Does not require a SORN. Provide explanation.
☒ Requires a new or additional SORN.
☐ Requires a modification to the following SORN(s):

Reason for Modifying SORN(s):

☐ A significant increase in the number, type, or category of individuals about whom records are maintained.
☐ A change that expands the types or categories of information maintained.
☐ A change that expands the types or categories of information maintained.
☐ A change that modifies the scope of the system.
☐ A change that modifies the purpose(s) for which the information in the System of Records is maintained.
☐ A change in the agency's authority to maintain the system, collect, use, or disseminate the records in the system.
☐ A change that modifies the way in which the system operates or its location(s) in such a manner as to modify the process by which individuals can exercise their rights under the statute.
☐ A change to equipment configuration (either hardware or software), storage protocol, type of media, or agency procedures that expands the availability of, and thereby creates substantially greater access to, the information in the system.
☐ The addition or rescindment of a Privacy Act exemption.
☐ A new routine use or significant change to an existing routine uses that has the effect of expanding the availability of the information in the system.

8. ANALYSIS OF PRIVACY RISK

8.1. PII Confidentiality Impact Level from NIST Special Publication 800-122

Indicate the potential impact/harm that could result to the subject individuals and/or DOL if PII were inappropriately accessed, used, or disclosed.

☐ **Low** – the loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.
☒ **Moderate** – the loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.
☐ **High** – the loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.

8.2. Identification and evaluation of potential risks to privacy

Adequacy of Privacy Training for DOL personnel

Privacy training for BLS personnel reinforces BLS's core value of protecting the privacy of our respondents and the confidentiality of their data. Required annual trainings, annual renewals of our pledges of adherence to BLS and DOL codes of conduct to uphold our fundamental responsibilities, all serve to reinforce and center our focus on privacy protection. In addition, the NLS program within BLS has 2 defined roles who have special responsibilities to oversee system privacy; they engage in additional trainings to develop and maintain their effectiveness. The NLS program also maintains close contact with BLS offices that provide technical support and advice.

RTI also emphasizes a strong commitment to protecting the privacy of individuals by requiring annual and periodic training programs. These include the basic training required of all BLS designated individuals (and endorsement of the BLS Code of Conduct) as well as specialized trainings required to maintain compliance with regulatory and contractual obligations (and adherence to RTI's own Code of Conduct). Ongoing participation in these trainings ensures that RTI staff are alert to the importance of privacy and able to identify and handle privacy risks effectively.

How Information is Acquired, Stored, and Shared

Data are collected directly from survey respondents. Survey data are stored in a secured physical location and encrypted per NIST SP 800-53 requirements and FIPS 140 standards. BLS and RTI will use data to conduct a survey and provide aggregate information to the public. BLS shares PII with RTI to conduct and improve the survey. BLS additional shares limited PII to a vendor for texting individuals regarding survey participation.

Describe the choices that were made with regard to preventing or mitigating these privacy risks

The NLSY27 employs robust security measures, including encrypted data transmission and secure, firewalled computing environments for data storage and analysis. This layered security approach minimizes the risk of unauthorized access. Access to sensitive data is strictly controlled through least privilege access, granting permissions only to officials who require access for their specific roles. These officials undergo comprehensive training in data privacy and are expected to uphold the BLS and DOL code of ethics. Regular assessments and updates of these practices help ensure that the NLSY27 remains compliant.

Protection against PII Breaches

Unauthorized Data Access:

PII is stored in a separate, encrypted database away from other survey responses. Confidential information is shared via Kiteworks to authorized RTI personnel. There is no third-party data sharing of NLSY27 Round 1 data by RTI. These data are owned exclusively by The Bureau of Labor Statistics (BLS) of the U.S. Department of Labor.

Potential Misuse of Data:

Only authorized BLS staff and RTI staff will have access to NLSY27 data consistent with their roles and responsibilities.

Protecting Against Insider Threats:

BLS utilizes least-privilege access, limiting the number of individuals who can access the system. The training documents and confidentiality certificates for designated RTI individuals are securely documented and updated as needed.

Describe the choices that were made with regard to preventing or mitigating these privacy risks

The NLSY27 system is tightly controlled to prevent unauthorized access, misuse of data, and insider threats, as detailed in the system's System Security and Privacy Plan (SSP) and in compliance with NIST Special Publication 800-53 and the Federal Information Security Modernization Act (FISMA). RTI annual staff trainings (Ethics, Confidentiality and Security) set clear performance expectations to prevent misuse of data. Trainings are tracked by RTI and typically involve quizzes that must be passed to ensure understanding and compliance comprehension. The NLSY27 System safeguards against insider threats in numerus ways by: 1) limiting access, 2) securely storing and encrypting separating PII from other survey data, 3) utilizing least privileged principles to staff that need to access PII for their role and survey responsibilities, 4) monitoring compliance and access, 5) use of crosswalk codes to minimize access to actual PII, and 6) not releasing PII beyond BLS officials.

Other:

N/A

Describe the choices that were made with regard to preventing or mitigating these privacy risks

N/A

Appendix 1. Artificial Intelligence (AI) and Machine Learning (ML)

To be completed by an information system that integrates an AI/ML component

Name the AI and or ML application?

Describe what the AI/ML is being used for?

Does the AI/ML component input, access, process, store, analyze, or generate outputs using any PII?

☐ Yes

☐ No

If yes, what PII elements are accessed, processed, or generated by the AI/ML component?

☐ Name/Former Name	☐ Date of Birth	☐ Maiden Name	☐ Place of Birth	☐ Citizenship
☐ Social Security number (including in truncated form)	☐ Driver's License	☐ Financial Account	☐ Taxpayer ID	☐ Passport Number
☐ Sex	☐ Telephone Number	☐ Criminal Record	☐ Education	☐ Age
☐ Financial Transaction	☐ Employer ID	☐ Alien Registration Number	☐ Vehicle Identifier	☐ Employee ID
☐ Credit Card	☐ Medical Record	☐ File/Case ID	☐ Financial Information	☐ Religion
☐ Alias	☐ Home Address	☐ Military Service	☐ Mother's Maiden Name	☐ Medical Information
☐ Email Address	☐ Marital Status	☐ Race/Ethnicity	☐ Occupation	☐ Work Email Address
☐ Job Title	☐ Salary	☐ Business Associates	☐ Work Telephone Number	☐ Proprietary or Business Information
☐ Employment Performance Ratings	☐ Work Address	☐ Work History	☐ Procurement or contracting records	☐ Other Performance Information
☐ Fingerprints	☐ Scars, Marks, Tattoos	☐ Signatures	☐ Photographs	☐ Palm Prints
☐ Hair Color	☐ Vascular Scans	☐ Weight	☐ Voice/Audio Recording	☐ Eye Color
☐ DNA Sample or Profile	☐ Dental Profile	☐ Video Recording	☐ Height	☐ Retina/Iris Scans

☐ User ID	☐ IP Address			
			☐ Other PII:	

Does the AI component transmit/maintain PII to any external systems, vendors, or cloud services?

How is PII protected when used by the AI/ML component?

SIGNATURE PAGE

Reviewed by: Julie Hatch Maxfield, Associate Commissioner BLS

JULIE MAXFIELD Digitally signed by JULIE MAXFIELD Date: 2026.04.08 14:50:30 -04'00'

Signature

Reviewed by: Muhammad Butt, Emerging Technology and Senior Advisor for Cybersecurity Initiatives OASAM-OCIO

MUHAMMAD BUTT Digitally signed by MUHAMMAD BUTT Date: 2026.04.09 09:17:16 -04'00'

Signature

Reviewed by: Mara Blumenthal , DOL Privacy Office OASAM-OCIO

MARA BLUMENTHAL Digitally signed by MARA BLUMENTHAL Date: 2026.04.08 11:52:15 -04'00'

Signature