U.S. Securities and Exchange Commission

Supplemental Health Benefits Program (SHBP)
PRIVACY IMPACT ASSESSMENT (PIA)

March 5, 2025

Office of Human Resources

Privacy Impact Assessment

Supplemental Health Benefits Program (SHBP)

Section 1: System Overview

1.1 Name of Project or System

Supplemental Health Benefits Program (SHBP)

1.2 Is the system internally or externally hosted?

☐ Internally Hosted (SEC)

☒ Externally Hosted (Contractor or other agency/organization) MetLife and Long Term Care Partners (LTCP)

1.3 Reason for completing PIA

☐ New project or system

☒ This is an existing system undergoing an update

First developed:

Last updated: 9/15/2016

Description of update: Updated for compliance with E.O. 14168

1.4 Does the system or program employ any of the following technologies?

☐ Electronic Data Warehouse (EDW)

☐ Social Media

☐ Mobile Application (or GPS)

☐ Cloud Computing Services

☒ Web Portal

☐ None of the Above

Section 2: Authority and Purpose of Collection

2.1 Describe the project and its purpose or function in the SEC's IT environment

Supplemental Health Benefits (SHBP) is a program that offers SEC employees additional benefits through SEC Select. Benefits include dental, vision, short and long term disability, and medical evacuation insurance. The Program is a collection of manual and automated processes supported by a suite of externally hosted web-based applications. In its rollout starting with the open enrollment season for 2016 benefits, MetLife will be the primary contractor and LTCP, a MetLife subcontractor, will host the website.

Plans offered through SEC Select will be administered through MetLife.

Employees will be able to access and select benefits through the SEC site administered by LTCP as well as a redirect to LTCP within the SEC network.

Census data needed to establish eligibility and facilitate the benefits election process will be provided to the SEC by the Department of the Interior (DOI). Each week, the SEC will pass that census data to LTCP via a secure connection.

As part of the 2015 SHBP rollout for 2016 coverage, employees will have access (from both inside and outside the SEC network) to an externally hosted web-based application.

The SEC Select Site: Employees will go directly to this site during benefits election open season to modify

coverage elections. Once enrolled, employees can view their elections & bi-weekly payroll deductions, view and edit their demographic information, make qualified life event (QLE) changes as well as access dental and vision network provider lookup functions, coverage information, claim forms and certificates of insurance. New employees will go directly to this site to choose their coverage.

In addition, at the employee's sole option, after an employee's MetLife benefits are active, he or she will be able to obtain customer service information on their MetLife coverage through the MetLife My Benefits Website (which is a website hosted by MetLife).

2.2 What specific legal authorities, arrangements, and/or agreements allow the information to be collected?

5 U.S.C. 302; 31 U.S.C. 3512

2.3 Does the project use, collect, or maintain Social Security numbers (SSNs)? *This includes truncated SSNs.*

☐ No
☒ Yes

If yes, provide the purpose of collection:	The SSN is needed by LTCP and MetLife. LTCP will use SSN for enrollment and billing purposes. MetLife will use SSN for insurance operations such as processing claims and providing customer service. The intended use is limited to treatment, payment and health care operations as permitted by HIPAA in order to administer benefit coverage.
If yes, provide the legal authority:	Executive Order 9397

2.4 Do you retrieve data in the system by using a personal identifier?

☐ No
☐ Yes, a SORN is in progress
☒ Yes, there is an existing SORN
SEC-15, Payroll, Attendance, Retirement and Leave Records.

2.5 Is the information covered by the Paperwork Reduction Act of 1995 (PRA)?

☒ No
☐ Yes

2.6 Considering the purpose of the collection, what privacy risks were identified and how were those risks mitigated?

The privacy risk is associated with the scope of the collection of information related to SEC employees and their family members. The privacy risks are mitigated by the vendor collecting the most sensitive information directly from the employee to provide the services requested. Also, on June 27, 2016, SHBP was granted an authorization to Use (ATU) by the SEC after a review of its Security Assessment and Authorization (SA&A) documentation completed by the Office of Personnel Management. Based on the security controls in place, the privacy risks are mitigated.

Section 3: Data Collection, Minimization, and Retention

3.1 What information is collected, maintained, used, or disseminated about individuals? *Check all that apply.*

☐ The system does not collect, maintain, use, or disseminate information about individuals.

Identifying Numbers

☒ Social Security Number	☐ Alien Registration	☐ Financial Accounts
☐ Taxpayer ID	☐ Driver's License Number	☐ Financial Transactions
☒ Employee ID	☐ Passport Information	☐ Vehicle Identifiers
☐ File/Case ID	☐ Credit Card Number	☐ Employer ID
☐ Other:		

General Personal Data

☒ Name	☒ Date of Birth	☐ Marriage Records
☐ Maiden Name	☐ Place of Birth	☐ Financial Information
☐ Alias	☒ Home Address	☐ Medical Information
☒ Sex	☐ Telephone Number	☐ Military Service
☐ Age	☒ Email Address	☐ Mother's Maiden Name
☐ Race/Ethnicity	☐ Education Records	☐ Health Plan Numbers
☐ Civil or Criminal History	☐ Zip Code	

☒ Other: Dependent's: name, date of birth, relationship to the employee, SSN, mailing address, and gender

Work-Related Data

☐ Occupation	☐ Telephone Number	☒ Salary
☒ Job Title	☒ Email Address	☒ Work History
☐ Work Address	☐ Certificate/License Number	☐ Business Associates
☐ PIV Card Information	☐ Fax Number	

☒ Other: Employee Organizational Code, Employee Appointment Type, Nature of Action Code, Employee Status History Type, Benefits Status Indicator, Benefits Status Effective Date, Plan Selections, and Bi-weekly Premium.

Distinguishing Features/Biometrics

☐ Fingerprints	☐ Photographs	☐ Genetic Information
☐ Voice Recording	☐ Video Recordings	☐ Voice Signature
☐ Other:		

System Administration/Audit Data

☐ User ID	☐ Date/Time of Access	☐ ID Files Accessed
☐ IP Address	☐ Queries Ran	☐ Contents of Files
☐ Other:		

3.2 Why the PII is listed in Question 3.1 collected, used, shared, or maintained by the system or project?

The PII is being collected in order to provide and administer supplemental health benefits to SEC employees. The data enables the SEC to adhere to the requirements of the SHB contract and comply with LTCP's carriers' legal obligation to accurately identify all persons that are covered. The system will collect data to support the SEC's offering and administration of supplemental health benefits to its employees. LTCP will use employee data (including PII) to support the process by which employees' select supplemental coverage. On a minimum necessary basis, enrollment information (including PII) will be securely transmitted to MetLife weekly for the sole purpose of MetLife's insurance operations (e.g., processing claims and providing customer service). To this end, "down-stream" systems, such as MetLife's claims processing, employee self-service, data warehousing and reporting systems will use the minimum necessary data to provide these insurance operation functions. Employee data in LTCP will also be accessed by OHR personnel and MetLife personnel who are administering the program.

3.3 Whose information may be collected, used, shared, or maintained by the system?

☒ SEC Employees
Purpose: To provide and administer supplemental health benefits

☐ SEC Federal Contractors
Purpose:

☐ Interns
Purpose:

☐ Members of the Public
Purpose:

☒ Employee Family Members
Purpose: To provide and administer supplemental health benefits

☐ Former Employees
Purpose:

☐ Job Applicants
Purpose:

☐ Vendors
Purpose:

☐ Other:
Purpose:

3.4 Describe the PII minimizing mechanisms and if the PII from the system is being used for testing, training, and/or research efforts.

The minimally necessary PII is collected directly from SEC Employees to receive the services they request. This information is not shared with the SEC staff. SEC will receive only ad hoc reports detailing statistical information on the participation by employees. Live (production) data is not used in any development, test, or training environments.

3.5 Has a retention schedule been established by the National Archives and Records Administration (NARA)?

☒ No.
The system will not maintain SEC records. Ad-hoc reports generated for the SEC will be maintained until they become inactive, at which time they will be retired or destroyed in accordance with records schedules of the SEC and as approved by the National Archives and Records Administration.

☐ Yes.

3.6 What are the procedures for identification and disposition at the end of the retention period?

Ad hoc reports will be disposed of using the procedures stated above.

3.7 Will the system monitor members of the public, employees, and/or contractors?

☒ N/A

☐ Members of the Public
Purpose:

☐ Employees
Purpose:

☐ Contractors

Purpose:

3.8 Considering the type of information collected, what privacy risks were identified and how were those risks mitigated?

The volume of information potentially collected by the system could pose privacy risks. Census information provided to the contract vendors by the SEC is limited to the information necessary about the employee. The most sensitive information about the employees and their family members are collected directly from the employee. Collecting the information from the individual employees directly reduces the risk of exposure to the information.

Section 4: Openness and Transparency

4.1 What forms of privacy notice were provided to the individuals prior to collection of data? *Check all that apply.*

☐ Privacy Act Statement

☒ System of Records Notice
SEC-15 "Payroll, Attendance, Retirement and Leave Records"

☒ Privacy Impact Assessment
Date of Last Update: 12/20/2010

☒ Web Privacy Policy
At point of login on the SEC Select site administered by LTCP

☐ Other notice:

☐ Notice was not provided.

4.2 Considering the method(s) of notice provided, what privacy risks were identified regarding adequate notice and how were those risks mitigated?

There is a privacy risk that employees may receive insufficient notice and/or an opportunity to make an informed decision to decline or consent to the information collected. To mitigate this risk, notice of the uses of information collected directly from SEC employees is provided at the point of collection on the SEC Select Site so that they may decide whether to provide the information. The site also allows employees to review their information, and edit it as necessary. Notice regarding information about employees provided by the SEC within the system has been addressed at the point of collection during the HR processes and in SORN SEC-15, Payroll, Attendance, Retirement and Leave Records.

Section 5: Limits on Uses and Sharing of Information

5.1 What methods are used to analyze the data?

N/A – The system does not conduct data analytics.

5.2 Will internal organizations have access to the data?

☐ No

☒ Yes

Organizations: OIT. The SEC implemented a data flow process to send SEC source files to LTCP. OIT support staff has limited access to the data flow process to troubleshoot any issues encountered with the SHBP data flow. LTCP on occasion may provide ad hoc statistical

reports to OHR regarding the level of participation of employees in the various benefit programs. To the extent there is any employee level reporting, OHR is provided the employee ID (ECI) only. OHR does not access the system and no PII is passed to them.

5.3 Describe the risk to privacy from internal sharing and describe how the risks are mitigated.

Since most of the information resides in the contractor hosted system the privacy risks for internal sharing are minimal. Access is limited to authorized personnel whose duties require access for purposes of troubleshooting.

5.4 Will external organizations have access to the data?

☐ No
☒ Yes

Organizations: LTCP only shares system data with MetLife per the controls required by the SEC SHBP Contract and federal law. Data will be shared with MetLife and downstream through MetLife's claim processing and customer service systems on a minimum necessary basis for the sole purpose of insurance operations. Data between DOI and SEC will be exchanged via a secure connection. Data between SEC and LTCP will be exchanged via a secure connection as well. Information needed by MetLife and down-stream systems (including VSP) are transmitted via a secure connection or from system to system within MetLife's network.

5.5 Describe the risk to privacy from external sharing and describe how the risks are mitigated.

Privacy risks associated with external sharing include risk of inadequate controls safeguarding the data and inappropriate access. SHBP only shares information with the external organizations required by the SEC SHBP Contract and are identified in this PIA. The organizations have limited access to fulfill its requirements under the contract and have in place approved security controls to protect the information collected.

Section 6: Data Quality and Integrity

6.1 Is the information collected directly from the individual or from another source?

☒ Directly from the individual.
☒ Other source(s): Information is collected from both source types. The DOI FPPS system will serve as the source of employee data for SHB.

6.2 What methods will be used to collect the data?

SEC OHR personnel use DOI's FPPS system to manage SEC employee payroll records. This includes the entry of all employee data that will be used in the SHBP data feed. DOI is using custom programming to extract the data needed to support the SHBP project. DOI will provide an updated file on every SEC employee on a weekly basis. The file will reside on the DOI secure server until an automated SEC process transfers the file over a secure data connection to a landing server, feeds server, etc.. The data connection is encrypted. The SEC transfers the census data to LTCP via Secure File Transfer Protocol (SFTP).

6.3 How will the data collected from individuals, or derived by the system, be checked for accuracy and completeness?

The DOI file is the master data for SEC employee information (name, DOB, SSN, etc.). Before loading the file for

transfer to the SEC, checks are done on the integrity and formatting of the data, to include: (1) ensuring new records (employees) are not loaded to the database unless all key information is included on the census file. This includes values for SSN, First Name, Last Name, Date of Birth, Salary, and mailing address information. This information is required to allow employees to activate an account and enroll in products that may require age and salary information to calculate premiums appropriately. (2) Checks for SSN records for an individual to prevent duplicate collections of the SSN. (3) Check to validate data stored is of the expected data type, allowable field lengths, and expected formatting of each data type.

The data received by the SEC from DOI is transferred over a secure data connection to SECFEEDS. The data connection uses Secure Copy (SCP) for encryption. The SEC transfers the census data to LTCP via Secure File Transfer Protocol (STFP).

LTCP receives a weekly Census file from the SEC. The census file is stored in a data directory reserved for the SHBP program. This data directory is locked down and only accessible by authorized production support staff. During the loading of the Census data to the database, checks are done on the integrity and formatting of the data prior to load. Once in the database, the data is subjected to quality control checks and referential constraints.

Data entered by users using the SEC Select Customer Service system (accessed by the call center representatives) or SEC Select site go through checks for data accuracy using formatting rules, the application rules engine, and referential constraints in the database before enrollee data can be saved. There also many control reports that are ran against the user enrollee and premium data. The customer service and enrollee portals only allow for secondary contact information to be added, enrollment selections (enroll, dis-enroll and QLE), and add or modify dependent information. All other data to support the SHB program comes from the census file and cannot be modified by the users or applications.

6.4 Does the project or system process, or access, PII in any other SEC system?

☒ No
☐ Yes.
System(s):

6.5 Consider the sources of the data and methods of collection and discuss the privacy risk for this system related to data quality and integrity? How are these risks mitigated?

There is a risk that information collected from multiple sources may not be accurate. This risk is mitigated since employees have access to the LTCP system and can correct the most sensitive information about them as necessary.

Section 7: Individual Participation

7.1 What opportunities are available for individuals to consent to uses, decline to provide information, or opt out of the project? If no opportunities are available to consent, decline or opt out, please explain.

The SEC provides initial employee data, including SSN, for all employees as part of the weekly census file transfer to LTCP. Providing employee data for all SEC employees is necessary to facilitate LTCP's carriers to comply with their legal obligation to accurately identify all persons that are covered. Employees may opt to not provide PII related to their dependents (spouse, child, etc.). However, failure to provide information requested may result in the denial of coverage for the dependents. Any personal data provided is used for benefits eligibility and claim processing only.

7.2 What procedures are in place to allow individuals to access their information?

Employees are able to access and select benefits through the externally hosted site administered by LTCP. The SEC has a site dedicated to SEC Select that has been programmed to redirect to the LTCP web-site.

7.3 Can individuals amend information about themselves in the system? If so, how?

Employees have access from both inside and outside of the SEC network to two externally hosted web-based applications. Employees cannot add to or overwrite the data received from the census file. This includes the following: SSN, Employee ID, Name, Gender, Date of Birth, Home Address, Primary Email Address, and Salary.

Employees can update the following: Employee's Secondary Email Address, Secondary Phone Number (Primary Phone Number is reserved in the event we receive this information on the census file), Dependent Information when applicable (First Name, Last Name, Date of Birth, Relationship to Employee, SSN, Mailing Address, Gender), and Plan Selections (enrollment in plans, beneficiary information if applicable).

7.4 Discuss the privacy risks related to individual participation and redress? How were these risks mitigated?

There are no privacy risks identified. Employees may edit the most sensitive information that they have provided at any time. Employee information provided in the census file may not be edited by the employee. However, the employee redress remedies are addressed in the source systems where the information was originally collected.

Section 8: Security

8.1 Has the system been authorized to process information?

☒ Yes
SA&A Completion Date: 2/1/2016
Date of Authority to Operate (ATO) Expected or Granted: 3/3/2016
☐ No

8.2 Identify individuals who will have access to the data in the project or system and state their respective roles.

☒ Users
Roles: All SEC employees will have access to the externally hosted web applications in order to manage their own individual benefits elections (and for their dependents) and monitor claims processing. Employees will only have access to their own information. The LTCP administrator has administrative level access to the LTCP-hosted system in order to troubleshoot employee questions and administer the program.

☒ Contractors
Roles: LTCP employees have access to an internally hosted customer service portal that is used to facilitate phone calls from the SEC employees. The customer service portal is role based and certain PII information is masked from view. Currently there are two roles in the SHB Customer Service portal. The CS Administrator role has access to setup and disable users, but has no access to any of the CS views and functionality. The CS Representative role has access to the views and functionality of the system, but no administrative privileges. All roles are controlled by the access management system AuthoTrack.

☐ Managers
Roles:

☐ Program Staff
Roles:

☐ Developers
Roles:

☒ System Administrators
Roles: System administrators will support the systems used by SHBP. Users of the systems consist of Federal employees and LTCP support personnel.

☐ Others:
Roles:

8.3 Can the system be accessed outside of a connected SEC network?

☐ No
☒ Yes

If yes, is secured authentication required?	☐	No	☐	Yes	☐	Not Applicable
Is the session encrypted?	☐	No	☒	Yes	☐	Not Applicable

8.4 How will the system be secured?

LTCP has administrative, technical, and physical safeguards in place to secure the system's data, to include: User roles that limit what information a user can access based on a "need-to-know"; information security policies and procedures for the safeguarding of the system data; required privacy training for employees on protecting PII and PHI; policies and procedures for the establishment, activation, modification, and termination of user accounts; audit trails of system events and user activity; and encryption methods implemented to protect data.

Specific details of LTCP safeguards are detailed below (redact this section before publication):

ADMINISTRATIVE CONTROLS

- Information Security Policies and Standards are NIST SP800-53R4 and HIPAA based.
- Dedicated Information Security Organization including a Security Council consisting of Senior Management.
- Employee Handbook covering employee responsibilities to protect customer PHI and PII.
- Regular externally performed security-based control assessments including compliance with FISMA, HIPAA, Data Privacy, SOX, SSAE16, and OWASP (aka web-site penetration tests).
- Regular internally performed security vulnerability scans, control surveys and audits including Key Risk Audit, Critical Data Asset Survey, SIG Survey (Shared Information Gathering Survey), Security Vulnerability Management Program.
- Information Technology based controls including Change Control Boards, Configuration Management, Patch Management, Performance Management, and Disaster Recovery Planning and Exercises.
- Business Continuity Planning and Exercises.
- Automated System and data access reviews performed quarterly by management (AuthoTrack)

AUTOMATED TECHNICAL CONTROLS WORKSTATION – DESKTOP, LAPTOP, THIN CLIENT

- Security Access Controls (AD/LDAP/Group Policy)
- Current anti-virus, anti-spam, malware protection (Sophos)
- Full Disk Encryption (Sophos)
- Session Timeout (Sophos)
- USB Ports Deactivated (Sophos)
- Standard password protected and encrypted USB Flash Drive (IronKey)
- Security vulnerability scanning (Nexpose)
- Security and operating system patching (Shavlik)

LAN

- Security Access Controls (AD/LDAP/Group Policy)
- Current anti-virus and malware protection (Sophos)

- Security vulnerability scanning (Nexpose)
- Security and operating system patching (Shavlik)

LAN-WAN
LAN controls mentioned above

- Firewalls, Intrusion detection and prevention (CISCO ASA, NetScaler-Web Application Firewall)
- Network device management (Solarwinds)
- Network Access Control (Forescout)
- Device monitoring – Denial of Service Protection (CISCO ASA)
- Website filtering (Websense)
- Email security and malware protection (IronPort)
- Security information and event management (ArcSight)

REMOTE ACCESS

- Encrypted Virtual Private Network (CISCO)
- Two-factor Authentication (RSA Token)
- Cell phone remote wipe management (ActiveSync)

APPLICATIONS

- Security vulnerability scanning including OWASP vulnerabilities (AppScan)

DATABASE

- Security Access Controls (AD/LDAP/Group Policy)
- Security vulnerability scanning (Nexpose)
- File Integrity Monitoring (Varonis)
- Encrypted Backups stored off-site (IBM TKLM)
- Real-time data replication (RecoveryPoint for infrastructure)
- Secured Portal for data exchange with OPM (SharePoint)

PHYSICAL CONTROLS

- Automated Physical Building Access Control (Facility Commander), and video camera surveillance
- Fire Suppression
- Uninterruptable Power Source (UPS) and Generator

8.5 Does the project or system involve an online collection of personal data?

☐ No
☒ Yes
Public URL: www.sec.gov/secselect

8.6 Does the site have a posted privacy notice?

☐ No
☒ Yes
☐ N/A

8.7 Does the project or system use web measurement and/or customization technologies?

☐ No
☒ Yes, but they do not collect PII

- Reports and Analytics - Adobe Analytics (Omniture Site Catalyst)
- Exact Target SalesForce Marketing Cloud,
- Google Analytics
  - We collect this web information to learn, assist and improve user experience.
  - This website utilizes website usage statistics to assist with improvements to our website and provide a better user experience. The multi-session web analytics tool employed doesn't collect

any personally identifiable information (PII). This technology anonymously tracks how visitors interact with this website and includes data regarding what sites referred visitors, what pages or files were accessed and what, if any, predetermined tasks were completed while visiting the site.

- The usage data collected by our website analytics tool aids optimization of the website by interpreting usage data we prioritize tasks, improve the website's user interface and tailor our content to that which most interests website visitors. No PII is collected via this technology so the anonymity of the end user remains protected. Any usage data collected will be retained only for as long as needed for analysis and optimization of the website and this information is accessible only to employees whose position requires it.

☐ Yes, and they collect PII

8.8 Describe any privacy risks for this system that relate to the technology and security of the system and how those risks are mitigated.

The privacy risks identified for this system is the potential for compromise if employee data to an unauthorized user or for an unauthorized purpose. This privacy risk is mitigated by the administrative, technical and physical Controls delineated in 8.4 above.

Section 9: Accountability and Auditing

9.1 Describe what privacy training is provided to users, either general or specific to the system or project.

All SEC employees and contractors receive annual privacy awareness training which outlines their roles and responsibilities for properly handling and protecting PII.

LTCP requires all LTCP associates (full-time employees, contractors, and temporary employees) to complete an annual training program that educates participants on safeguarding PII and PHI in all forms (e.g., hardcopy, electronic, and verbal) and describes the Clean Desk Policy for the securing of hard copy and electronic information. LTCP strictly grants access to PII and PHI on a must know or necessary-for-the-job basis with quarterly reviews of access by each manager.

LTCP also delivers incident reporting and response training that includes handling of potential PII and PHI data exposure to all managers and supervisors to ensure proper procedures are followed.

It is standard business process for all MetLife associates to undergo mandatory Privacy, Information System Security Awareness Training, and other HIPAA Privacy awareness training courses, which include comprehension testing at the end of the training. Lists of all associates who have completed the training are maintained in the Compliance Department with communication to managers to ensure that all users have successfully completed training.

9.2 Does the system generate reports that contain information on individuals?

☒ No

☐ Yes

There are no reports generated automatically from the system. Authorized business analysts pull data from the system to provide enrollment statistics, and periodically ad hoc reports are requested by the SEC. Ad hoc reports typically only leverage Employee ID (no PII), however, there could be a need based on the request to occasionally to provide employee first name, and/or last name, and/or email address.

9.3 Do contracts for the system include Federal Acquisition Regulation (FAR) and other applicable clauses ensuring adherence to the privacy provisions and practices?

☐ No
☒ Yes
☐ This is not a contractor operated system

9.4 Does the system employ audit logging or event logging?

☐ No
☒ Yes

Yes the system logs are sent to the SIEM (Security information and event management) tool (ArcSight). Any issues will trigger alerts to IT and Information Security teams, and the reports are reviewed monthly. Application transactions/events generated by the system are stored in the database and control reports are generated on the events, and these reports are reviewed daily, weekly, and monthly. The system also employs many other monitoring systems for uptime, response times, and resource utilization and these systems generate real time alerts and are reviewed monthly.

9.5 What auditing measures/controls and technical safeguards are in place to prevent misuse (e.g., unauthorized browsing) of the data? What mechanisms are in place to identify security breaches?

The NIST 800-53 Security Control AC-5 requires the organization to separate employee duties, document such separation, and define a level of information system access that supports such separation of duties. This control is intended to prevent employees from potentially abusing a high level of system access or from colluding to perform malevolent systems activity. To provide such protection, LTCP must adequately audit and control the extent to which its employees can access PII/PHI information or business critical systems. LTCP's AuthoTrack is an internally developed auditing mechanism, with a simple web interface, used to grant and monitor an employee's access level to various LTCP systems, including those that store PHI/PII information and those that provide critical business functions.

9.6 Given the sensitivity of the PII in the system, manner of use, and established safeguards, describe the expected residual risk related to access.

Based on the technical, administrative, and physical controls described in the PIA, the privacy risks to the information collected has been mitigated to minimal risk. There are no expected residual risks identified.