Privacy Impact Assessment
for the

ANNUITANT HEALTH BENEFITS OPEN SEASON SYSTEM

August 29, 2012

Contact Point

Woody Klinger
Chief, Retirement Eligibility and Services

Reviewing Official

Matthew E. Perry
Chief Privacy Officer
U.S. Office of Personnel Management

SECTION 1: Privacy Impact Assessment (PIA) SUMMARY INFORMATION

a. Overview

The Annuitant Health Benefits Open Season System (AHBOSS) is a tool used, during the annual Federal Employees Health Benefits Open Season, to support the mission of the Retirement Eligibility and Services, Retirement Benefits Branch. This tool has both a website and Interactive Voice Response (IVR) application that annuitants use to make health benefit enrollment changes and/or to request brochure information for plans participating in the Federal Employees Health Benefits (FEHB) Program during the annual open season enrollment period. The data stored in this application is subject to the Privacy Act. Information collected by this system includes Name, Social Security Number, Mailing Address, Current Health Plan, Claim Number, Date of Birth, Marital Status, Gender, Carrier Control Number, Email Address, and dependent information, if applicable. Web interaction transcripts that may contain some of this data are also stored. Automated email transactions are initiated by the system and are distributed by Leepfrog Technologies, Inc., a contracted vendor. Annuitants use the AHBOSS to initiate their enrollment change for the upcoming year. An annuitant provides his or her identifying information to start the process. Website users enter identifying information once to create a personal account with an annuitant defined user name and masked password. The username and password are also stored by AHBOSS and are used to authenticate users for subsequent web access during the current open season. Both the website and the IVR allow transactions including information requests and enrollment changes for authenticated users. Files containing address and request information is passed to a contracted third party, SourceHOV, for fulfillment. Brochure requests are handled by SourceHOV staff with OPM security clearances that assemble and mail the health benefit carrier plan brochures. Enrollment change requests are stored in AHBOSS during Open Season and are submitted to OPM for updates. Two update enrollment transactions files are electronically sent to OPM. One file is sent to the OPM, Chief Information Officer, Operations Technology Management, Data Center, and the second file is sent to the Human Resources Solutions, Human Resources Management Solutions, Human Resources Tools and Technology. The file transmission to the Data Center updates the retirement legacy system and the file sent to Human Resources Tools and Technology sends the new enrollment information to both the new and old FEHB plan. All transactions processed through this site are encrypted and electronically transmitted to Office of Personnel Management (OPM) daily using encrypted file transmission. The legal authority for maintenance of the system includes the following with any revisions or amendments: Section 3301 and chapters 83, 84, 87, 89 of title 5, United States Code, Pub. L. 83–598, 84–356, 86–724, and 94–455; and Executive Order 9397.

The system modifications from September 2012 include the following:
1. Address Verification Agent: The address verification agent introduces an address validation tool that looks for invalid addresses and converts the addresses into valid, functional United States Postal Service (USPS) addresses, or flags them as invalid. This includes the usage of the annuitant's mailing addresses. The addresses are originally provided by the annuitants.
2. Data Entry Screens: The data entry screens include new Graphical User Interface (GUI) screens that allow the input of family enrollment and direct pay letter information. The information is considered of moderate sensitivity.
3. Password Management Procedure: This module sends a temporary password to an annuitant who has forgotten their password. The password is sent to the email address on file. The user then accesses the AHBOSS system with the temporary password and is prompted for a new password. After the new password is entered, the temporary password is disabled and the new password becomes active. Sensitive information included in the "Password Management Procedure" is the temporary password.

4. Mobile Application: The Mobile Application modification produces a mobile directory and presents a GUI interface for smart phone devices. There is no new functionality or sensitive data that is introduced by this modification.

b. Why is this PIA being created or updated? Choose one:

☐ **New OPM Information System**	☐ **New Electronic Collection**
☒ **Existing OPM Information System**	☐ **Existing Electronic Collection**
☐ **Significantly Modified OPM Information System**	

c. Does the OPM information system or electronic collection have a Privacy Act System of Records Notice (SORN)?

NOTE: A Privacy Act SORN is required if the information system or electronic collection contains information about U.S. citizens or lawful permanent U.S. residents that is retrieved by name or other unique identifier. PIA and Privacy Act SORN information should be consistent.

☒ **Yes** **Enter Privacy Act SORN Number/Name** OPM, Central-1 Civil Service Retirement and Benefits Records.

or

☐ **No** **Date of submission for approval to OPM Privacy Office**
Consult the Privacy Office for this date.

d. Summary of OPM information system or electronic collection. Answers to these questions should be consistent with security guidelines for release of information to the public.

(1) Describe the purpose of this OPM information system or electronic collection and briefly describe the types of personal information about individuals collected in the system.

Information is collected to complete health benefit enrollment changes and to send plan brochures based on requests from civil service retirees and survivor annuitants. The enrollment changes are processed to update the annuitants' records in OPM's legacy retirement systems. Web account information is used to authenticate and then grant annuitants access to web functionality. Transactional information, interaction channel and request types with counts, are used to manage staffing and services for program operations. Information collected and used by this system includes Name, Social Security Number, Mailing Address, Health Insurance Plan Information, Claim Number, Data of Birth, and Email Addresses for civil service retirees and their survivors. Upon election, Name, Social Security Number, and Date of Birth is also collected and retained for annuitant spouses, dependents, and legal beneficiaries. . For website users, user names and passwords are also collected and maintained for annuitant use during Open Season. Managerial reports tracking request types and volumes for the current season are also generated and provided to OPM. Webmail and web chat communication records are also collected and stored.

The system modification, "Data Entry Screens" includes new GUI screens that allow the input of family enrollment and direct pay letter information.

(2) Briefly describe the privacy risks associated with the Personally Identifiable Information (PII) collected and how these risks are addressed to safeguard privacy.

The privacy risk from the information sharing is inadvertent/unintentional disclosure of PII and a breach of contractor system. These risks are mitigated by a variety of system security controls including, Access and Account Management, Security and Privacy Awareness Training, Auditing and Audit Review, Information Systems Backups, Incident Response and Incident Response Training, Media Protection, Personnel Security Screenings, Separation of Duties, Least Privilege, Boundary Protection, System Communications Protections, and Interconnection Service Agreements, governing the security requirements for data exchanges. Vangent's management of the system is overseen through authorization assessments of security controls to determine if they are in place and operating as intended, as well as continuous monitoring. Operationally, Vangent personnel are restricted from sensitive information gathered using Access and Account Management, Auditing and Audit Review, Least Privilege, and System Communications Protection controls. In addition, each Vangent contractor is only provided with the minimum data necessary to process health benefit open season enrollment changes. Additional controls on Verizon Business, SourceHOV, and Leepfrog Technologies include System and Services Acquisition Controls, Systems Communications Protections, Boundary Protection, Interconnection Security Agreements, and Personnel Security Screenings.

For the "Data Entry Screens" system modification, sensitive data includes the entry of family enrollment and direct pay letter information.

e. Retention of Information. Does this information system or electronic collection retain information?

☒ **Yes**

Information Retained	Information retained by AHBOSS includes Name, Social Security Number, Mailing Address, Health Insurance Information (plan code and premium amount), Claim Number, Date of Birth, and Email Addresses for civil service retirees and their survivors. Upon election, Name, Social Security Number, and Date of Birth are also retained for annuitant spouses, dependents, and legal beneficiaries. For website users, user name, and password are retained as well as webmail and web chat communication records. The number and type of each transaction by interaction channel (i.e. phone) is also stored.
Time period for retained information	Both AHBOSS health benefit enrollment information and web account information are retained for one year while spouse and/or dependent data gathered is retained from year to year. Paper-based retirement records are retained for 115 years from date of the employee's birth or 30 years after the date of employee's death, if no application for benefits is received as referenced in OPM's Records Handbook 3 Ret.01.
Retention Schedule Name	Currently pending.

☐ **No**

f. Authority to collect information. A Federal law, Executive Order of the President (EO), or OPM requirement must authorize the collection and maintenance of a system of records.

The legal mechanism that the information technology (IT) system is allowed to share information in identifiable form or personally identifiable information outside of OPM is the System of Records Notice, OPM, Central-1 Civil Service Retirement and Benefits Records.

The legal authority for retirement health benefits includes the following with any revisions or amendments: Section 3301 and chapters 83, 84, 87, 89 of title 5, United States Code, Pub. L. 83–598, 84–356, 86–724, and 94–455; and Executive Order 9397.

g. Information Retrieval. How is the information retrieved? (By name, SSN, etc)

Information about an annuitant can be retrieved by one of the following:

a. claim number
b. social security number
c. first and last name and mailing address

h. With whom will the PII be shared through data exchange, both within OPM and outside OPM (e.g., other Federal Agencies)? Indicate all that apply.

☒ **Within OPM. Specify**

Program Offices and IT systems within OPM with which personal and benefits information from the ABOSS is shared:

a. Retirement Services
b. Chief Information Officer (CIO), Data Center and Benefits Systems; and,
c. Human Resources Solutions, Human Resources Tools and Technology

The information used to process enrollment changes is shared with the health benefit carriers participating in the FEHB Program. The information would be used in the Chief Information Officer to update existing annuity records if enrollment changes are made. The purpose is to inform new and old carrier for the enrollment change and health benefit premiums deductions.

☐ **Other Federal Agencies. Specify** (agencies, not systems)

None

☐ State and Local Agencies. **Specify** (agencies, not systems)

None

☒ Contractor **(enter name and describe the language in the contract that safeguards PII.) Specify**

Vangent has access to this information since they are the external organization contracted to manage the AHBOSS applications. Verizon Business is contracted by Vangent to host Vangent IT systems and maintain privileged access to servers that host information. Leepfrog Technologies, Inc. is contracted by Vangent to send emails to annuitants and, therefore, has access to annuitant names and email addresses. Similarly, SourceHOV, Inc. is contracted by Vangent to send mailings and has access to names and street addresses. As a part of OPM's Retirement Information Office contracted customer support, Spherix, Inc. employees also have access to AHBOSS information.

File sharing data between OPM, Vangent, Leepfrog Technologies, Inc., and SourceHOV is outlined in the Interconnection Security Agreements (ISA's) for the AHBOSS. Controls governing this sharing include Access and Account Management, Security and Privacy Awareness Training, Auditing and Audit Review, Personnel Security Screenings, Boundary Protection, and File Encryption. Controls governing Verizon Business hosting include Access and Account Management, Auditing and Audit Review, Personnel Security Screenings, Boundary Protection, System and Services Acquisition Controls, and Least Privilege.

To view the Vangent contract verbiage with OPM, reference Appendix A: Contract Verbiage.

☒ Other **(e.g., commercial providers, colleges). Specify**

Leepfrog provides emailing services for annuitants. SourceHOV provides print services for annuitants. Verizon provides system administration services.

i. Do individuals have the opportunity to object to the collection of their PII?

☒ **Yes** ☐ **No**

(1) If "Yes," describe the method by which individuals can object to the collection of PII.

Annuitants may decline to provide the information. The Privacy Act and Public Burden Statements inform annuitants that the requested information is necessary to process health benefit enrollment change request. There is no penalty for maintaining the same health benefit plan year to year. They can elect to keep their current health benefit carrier, preventing the need for existing data collection.

(2) If "No," state the reason why individuals cannot object.

j. Do individuals have the opportunity to consent to the specific uses of their PII?

☒ **Yes** ☐ **No**

(1) If "Yes," describe the method by which individuals can give or withhold their consent.

The AHBOSS includes a notice on the tools website and IVR prior to collecting information and warns webmail and web chat users not to disclose PII through a notification banner. Annuitants are also informed that Office of Management and Budget (OMB) has approved the collection of information and the associated OMB approval number for the website is 3206-0201 and a screen shot of the screen has been attached. The IVR OMB approval number for the IVR is currently in the clearance process. The Privacy Act and Public Burden Statements are also provided. This is sufficient since it informs the public of why the information is being collected and they can choose whether to submit a health benefit plan open season change request. The SORN is OPM, Central-1.

All information is collected for the purpose of assisting annuitants in the annual selection of health benefits. By providing information, annuitants are expressing consent that the data be used for this single purpose.

The Privacy Act and Public Burden Statements and OMB clearance numbers are posted at the AHBOSS website and also provided prior to IVR data collection. Risks associated to individuals being unaware of the data collection are mitigated by providing the Privacy Act and Public Burden Statements, established SORN, and the OMB clearance number authorizing the collection and its usage.

(2) If "No," state the reason why individuals cannot give or withhold their consent.

k. What information is provided to an individual when asked to provide PII data? Indicate all that apply. When collecting information from an individual, either in a paper or electronic collection, individuals have a right to understand the authority, purpose, routine uses that apply and the effects on the individual.

☒ **Privacy Act Statement**

☐ **Privacy Advisory**

☒ **Other**

☐ **None**

Describe each applicable format.

The Privacy Act and Public Burden Statements and OMB clearance numbers are posted at the AHBOSS website and also provided prior to IVR data collection. Risks associated to individuals being unaware of the data collection are mitigated by providing the Privacy Act and Public Burden Statements, established SORN, and the OMB clearance number authorizing the collection and its usage.

SECTION 2: PIA QUESTIONNAIRE and RISK REVIEW

a. For the questions in subparagraphs 2.a.(1) through 2.a.(5), indicate what PII (a data element alone or in combination that can uniquely identify an individual) will be collected and describe the source, collection method, purpose, and intended use of the PII.

(1) What PII will be collected? Indicate all individual PII or PII groupings that apply in the table below.

Non-Sensitive PII		
☒Name	☐Other Names Used	☐Marital Status
☐Work Cell Telephone Number	☐Work Telephone Number	☐Work Email Address
☐Emergency Contact	☐Salary	
Sensitive PII		
☒Social Security Number (SSN)	☐Truncated SSN	☐Driver's License
☐Personal Cell Telephone Number	☐Home Telephone Number	☐Other Identification (ID) Number
☐Citizenship	☐Legal Status	☐Gender
☐Race/Ethnicity	☒Birth Date	☐Place of Birth
☐Mother's Maiden Name	☐Mother's Middle Name	☐Security Clearance
☒Personal Email Address	☒Mailing/Home Address	☐Spouse Information
☐Financial Information	☐Medical Information	☐Biometrics
☐Law Enforcement Information	☐Employment Information	☐Disability Information
☐Child Information	☐Education Information	☐Military Records
		☒Other

If "Other," specify or explain any PII grouping selected.

Health Insurance Plan Information, Claim Number, usernames, passwords, webmail, web chat communication records

(2) What is the source for the PII collected (e.g., individual, existing OPM information systems, other Federal information systems or databases, commercial systems)?

Describe.

Information for the AHBOSS is provided via a data file electronic transmission from OPM. Information is also gathered from annuitants. Management reports are also generated for OPM Retirement Services. These reports provide metrics to track the number of requests as well as type of health benefit open season request.

For the system modification, "Data Entry Screens" (Sept. 2012), the source of information collected is from the annuitants.

How will the information be collected? Indicate all that apply.

- ☐ Paper Format
- ☒ Telephone Interview
- ☒ Email
- ☒ Information Sharing from System to System
- ☒ Other (Describe)
- ☐ Face-to-Face Contact
- ☐ Fax
- ☒ Web Site

Note: Email is collected through webmail.

(3) Why are you collecting the PII selected (e.g., verification, identification, authentication, data matching)?

Describe

Information is collected to support the mission of administering the FEHB program for civil service annuitants in accordance with Section 3301 and chapters 83, 84, 87, 89 of title 5, United States Code, Pub. L. 83–598, 84–356, 86–724, and 94–455; and Executive Order 9397.

(4) What is the intended use of the PII collected (e.g., mission-related use, administrative use)?

Describe

Information is collected to complete health benefit enrollment changes and to send plan brochures based on requests from civil service retirees and survivor annuitants. The enrollment changes are processed to update the annuitants' records in OPM's legacy retirement systems. Web account information is used to authenticate and then grant annuitants access to web functionality. Transactional information, interaction channel and request types with counts, are used to manage staffing and services for program operations.

b. Does this OPM information system or electronic collection create or derive new PII about individuals through data aggregation? (See Appendix for data aggregation definition.)

☐ **Yes**

☒ **No**

If "Yes," explain what risks are introduced by this data aggregation and how this risk is mitigated.

c. Who has or will have access to PII in the OPM information system or electronic collection? Indicate all that apply.

☒ **Users** ☒ **Developers** ☒ **System Administrators** ☒ **Contractors**

☒ **Other** (Describe)

Users will have access to their own PII only.

d. How will the PII be secured?

(1) Physical Controls. Indicate all that apply.

☒ Security Guards
Identification Badges

☐ Cipher Locks

☐ Combination Locks
Closed Circuit Television

☒ Key Cards

☐ Safes

☒ Other (Describe)

Closed Circuit Television

(2) Technical Controls. Indicate all that apply.

- ☒ User Identification
- ☒ Password
- ☐ Intrusion Detection System (IDS)
- ☒ Encryption
- ☐ External Certificate Authority (CA) Certificate
- ☒ Other (Describe)
- ☐ Biometrics
- ☒ Firewall
- ☒ Virtual Private Network (VPN)
- ☐ Public Key Infrastructure Certificates

An Intrusion Prevention System (IPS) can prevent attacks on the network. An Intrusion Detectino System (IDS) only detects network attacks.

(3) Administrative Controls. Indicate all that apply.

- ☒ Periodic Security Audits
- ☐ Regular Monitoring of Users' Security Practices
- ☒ Methods to Ensure Only Authorized Personnel Access to PII
- ☐ Encryption of Backups Containing Sensitive Data
- ☒ Backups Secured Off-site
- ☒ Security and Privacy Awareness Training
- ☒ Other (Describe)

Domain policy, access control lists, patching processes, least privilege. Auditing controls are implemented for analysis and review.

e. Does this OPM information system require an authorization and assessment under the OPM Authorization and Assessment Process?

☒ **Yes.** Indicate the certification and accreditation status:

☒ Authorization to Operate (ATO) Date Granted: November 2011

☐ Denial of Authorization to Operate (DATO) Date Granted:

☐ Limited Authority To Operate (LATO) Date Granted:

☐ **No**, this OPM Information system does not require an authorization and assessment.

f. How do information handling practices at each stage of the "information life cycle" (i.e., collection, use, retention, processing, disclosure and destruction) affect individuals' privacy?

Describe.

Individual's privacy at each stage of the "information life cycle" is restricted by least privilege. Users are given read/write privileges based on the requirements to execute his or her job requirements. At the collection phase, the information is sent through a secure connection and stored in a database that is located behind the Internet firewall. At the "use" phase, only federal employees and contractors with security clearance have access to the data. At the retention phase, the database is restricted to authorized users and backed up on internal network servers. At the processing phase, the information is modified and updated on the database. For disclosure, the information can only be disclosed by users that have username and password access to the web server. For destruction, reference item "e." for data

g. For existing OPM information systems or electronic collections, what measures have been put in place to address identified privacy risks?

Describe:

The Annuitant Health Benefits Open Season System is subject to continuous monitoring, including n annual security assessments and tri-annual authorization assessments, under OPM IT Security and Privacy Policy and based on guidance from the National Institute of Standards and Technology and other relevant requirements regarding Information Technology security and privacy.
OPM's Inspector General may also conduct periodic reviews. The transfer of information is restricted by a secure link from the user to the web server. The database server with PII is with restricted access controls on the operating system and on the database. .

For the September 2012 modifications, the modifications will rely on the existing information security controls on the servers and network. This will include the firewall, Intrusion Detection and Prevention (IDP), operating system controls, and database controls. The "Password Management Procedure" will introduce a new

h. For new OPM information systems or electronic collections, what measures are planned for implementation to address identified privacy risks?

Describe.

The Annuitant Health Benefits Open Season System is subject to continuous monitoring, including n annual security assessments and tri-annual authorization assessments, under OPM IT Security and Privacy Policy and based on guidance from the National Institute of Standards and Technology and other relevant requirements regarding Information Technology security and privacy. Any identified vulnerabilities are tracked for mitigation.

SECTION 3: REVIEW AND APPROVAL SIGNATURES

Prior to the submission of the PIA for review and approval, the PIA must be coordinated by the Program Manager or designee through the OPM Privacy Officer prior to being signed by the system owner, Chief Information Security Officer (CISO) or CIO.

System Owner

Signature: 1-30-2013

Name: Woody E. Klinger

Organization: U.S. Office of Personnel Management, Retirement Services, Retirement Operations, Retirement Eligibility and Services

Email Address: woody.klinger@opm.gov

Date of Review:

Chief Information Security Officer

Signature:

Name: Andy Newton

Organization: Office of the Chief Information Officer

Email Address: andy.newton@opm.gov

Date of Review: 2/6/2013

Chief Privacy Officer

Signature:

Name: Matthew E. Perry

Organization: Office of the Chief Information Officer

Email Address: matthew.perry@opm.gov

Date of Review: 2/6/2013

APPENDIX A: CONTRACT VERBIAGE

1752.224-70 Protecting Personally Identifiable Information

(a) Applicability

This clause applies to contractor personnel and addresses specific OPM requirements in addition to those included in the Privacy Act of 1974 (5 U.S.C. 552a - the Act). The following should not be construed to alter or diminish civil and/or criminal liabilities provided under the Act.

(b) Definition of Personally Identifiable Information (PII)

Personally Identifiable Information (PII) is "information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc. alone or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc." (http://www.whitehouse.gov/omb/memoranda/fy2007/m07-16.pdf). In other words, **PII** refers to **any information**, on **any medium**, that **identifies a specific individual** whether the information is on paper or electronic.

(c) Responsibilities for Handling PII

(1) Contract employees shall not remove PII from their individual assigned duty station without prior approval of their supervisor.

(2) All contract employees are personally responsible for the proper handling of PII, regardless of location. All contract employees must be:

- responsible for the proper control and handling of PII residing on their computer, on removable media, and on paper documents.
- responsible for ensuring portable data storage and communication devices are properly controlled and secured at all times.
- responsible for the proper marking, control and storage of printouts and other paper documents containing PII in their possession.
- Email cannot be encrypted. Since PII must be encrypted before being sent, send it only as an encrypted attachment. Do not send PII in the content of an email.

(d) Encryption of Personally Identifiable Information (PII)

(1) OPM has a policy protecting, and when appropriate, restricting sending, copying or moving PII from the OPM network. Therefore, if the contract employees must send PII, send it only as an encrypted attachment. OPM employees and contractors are required to encrypt PII data using WinZip. Instructions on how to use WinZip to encrypt and protect files containing PII are available on Theo at: http://theo.opm.gov/helpdesk/selfhelp/WinZipv90EncryptionProcedures.pdf. WinZip can be used to protect data on workstations, laptops and email attachments. It is available on all OPM workstations attached to the agency's network.

(2) A password protected file is not secure. Never send any unencrypted PII data in e-mail.

(e) Procedures for Reporting a Breach of PII

(1) A breach of PII includes loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or unauthorized access of personally identifiable information whether physical or electronic. As an agency, OPM is required to immediately report all potential PII data breaches -- whether they involve paper documents or electronic information. In order to meet this responsibility, OPM has established a new internal procedure for reporting the loss or possible compromise of any PII, and this clause conforms to that procedure.

(2) OPM contractors must report any breach or potential breach to the OPM Situation Room and the Contracting Officer within 30 minutes of becoming aware of the risk – regardless of the time or day of the week. Breaches should be reported, even if it is believed the breach is limited, small, or insignificant. OPM's IT security experts, who will determine when a breach needs additional focus and attention. The OPM Situation Room is available 24 hours per day, 365 days per year. Report the breach to the OPM Situation Room and the Contracting Officer either by phone or by e-mail; however, be sure NOT to include PII in the e-mail.