



# EXCHANGE

## PRIVACY IMPACT ASSESSMENT (PIA)

AAFES eBenefits (Willis Towers Watson)

AAFES Financial Benefits Development and Administration

Questions relative to this document should be directed to the Exchange Office of General Counsel, Compliance Division, ATTN: Privacy Manager by mail to 3911 S. Walton Walker Blvd., Dallas, TX 75236 or through e-mail to PrivacyManager@aafes.com.

**OBJECTIVE:** The objective of a PIA is to determine the scope, justification, and Privacy Act applicability for systems collecting, storing, or processing sensitive, personal data that may be concerned to be private. **A PIA should be completed prior to development/procuring any new IT system which collects/maintains such information or updated when a significant change is made to the system.** The OGC-C Privacy Manager for the Exchange will track, monitor, and approval all finalized PIA and compliance with the E-Government Act of 2002. Completed and approved PIAs will be forwarded to the system owner and to the IT-Government (IT-G) representative.

### SECTION 1: IS A PIA REQUIRED?

**A. Will this Exchange information system or electronic collection of information collect, maintain, use, and/or disseminate Personal Identifiable Information (PII) about members of the public, federal personnel, contractors or foreign nationals employed at U.S. military facilities internationally? (Mark all that apply).**

Members of the General Public.

Foreign Nationals

Federal Personnel / Exchange Associates

Federal Contractors and/or Vendors

**B. If no items are marked in question A, you may stop here. Have this PIA signed and return it to the Privacy Manager.**

**C. If any item in A is marked, proceed to Section 2.**

**SECTION 2: PIA SUMMARY INFORMATION**

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

- New Information System
- New Electronic Collection
- Existing Information System
- Existing Electronic Collection
- Significantly Modified Information System

If unsure, consult OGC-C Privacy Manager.

**B. Does this information system or electronic collection require a Privacy Act System of Records Notice (SORN)? [if unknown, please contact OGC-C]**

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
- No, a SORN is not required for this system.

If "Yes," enter Privacy Act SORN Identifier

AAFES 0703.07

Date of submission for approval to Defense Privacy Office  
Consult the OGC-C Privacy Manager for this date.

February 2017

**C. Does this information system or electronic collection have an Office of Management & Budget (OMB) Control Number? [if unknown, contact OGC-C Privacy Manager].**

- Yes

Enter OMB Control Number

0702-0139

Enter Expiration Date

September 30, 2019

- No

**D. Authority to collect information. Please list the Federal law, Executive Order of the President (EO), or regulation which authorizes the collection and maintenance of a system of records. [if unknown, contact OGC-C Privacy Manager]**

(1) If this system has a Privacy Act SORN, the authorities in this PIA and the existing Privacy Act SORN should be the same.

(2) Cite the authority for this information system or electronic collection to collect, use, maintain and/or disseminate PII. (If multiple authorities are cited, provide all that apply.) i.e. Title 10 U.S.C. § 7013, "Secretary of the Army".

(a) Whenever possible, cite the specific provisions of the statute and/or EO that authorizes the operation of the system and the collection of PII.

(b) If a specific statute or EO does not exist, determine if an indirect statutory authority can be cited. An indirect authority may be cited if the authority requires the operation or administration of a program, the execution of which will require the collection and maintenance of a system of records.

(c) The Exchange may use Exchange Operating Procedures, Exchange Standards of Operations, or CEO Guidance as the primary authority. The requirement, directive, or instruction implementing the statute within the Exchange should be identified.

10 U.S.C. 7013, Secretary of the Army; 10 U.S.C. 9013, Secretary of the Air Force; 42 U.S.C. 659, Consent by United States to Income Withholding, Garnishment, and Similar Proceedings for Enforcement of Child Support and Alimony Obligations; 31 CFR 285.11, Administrative Wage Garnishment; DoD Directive 7000.14-R, DoD Financial Management Regulation; DoD Instruction 1400.25, Volume 1408, DoD Civilian Personnel Management System: Insurance and Annuities for Nonappropriated Fund (NAF) Employees; Army Regulation 215-8/AFI 34-211(I), Army and Air Force Exchange Service Operations; and E.O. 9397 (SSN), as amended.

**E. Summary of 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 information system or electronic collection.

To process benefits, answer inquires and process claims.

(2) Briefly describe the types of personal information about individuals collected in this system.

Employee's, spouse's or former spouse's, beneficiaries', and children's, full name, social security number (SSN), address, gender, date of birth, marital status, telephone number (home/cell/work), e-mail address; employee's number of dependents, pay, withholding/deduction authorization for health benefits, life insurance, benefit plan participation data, job code and title, employment category, base hourly rate, court orders affecting benefit enrollment, and change forms to include health, dental, flexible spending, disability, life insurance; employee's or beneficiaries' financial institution name and routing number; tax exemption certificates; statistical reports relating to benefits.

(3) Briefly describe the privacy risks associated with the PII collected and how these risks are addressed to safeguard privacy.

The main risk is data leakage. Records are maintained in a controlled facility. Physical entry is restricted by the use of locks, guards, and is accessible only to authorized personnel. Access to records is limited to person(s) with an official "need to know" who are responsible for servicing the record in performance of their official duties. Persons are properly screened and cleared for access. Access to computerized data is role-based and further restricted by passwords, which are changed periodically. In addition, integrity of automated data is ensured by internal audit procedures, data base access accounting reports and controls to preclude unauthorized disclosure.

**F. With whom will the PII maintained in this system be shared? (i.e., other DoD Components, Federal Agencies)?** Indicate all that apply. Questions should be coordinated with OGC-C Privacy Manager.

**Within the Exchange.**

Specify. Financial Associates in Benefits Development & Administration; Human Resource Staff, Attorney Staff, Loss Prevention, Inspector General, Hearing Examiner, EEOC

**Other DoD Components.**

Specify. Dept. of the Army, Dept. of Air Force, Army and Air Force IG office

**Other Federal Agencies.**

Specify. Dept. of Justice; U.S. Treasury; U.S. DOL, Dept. of State

**State and Local Agencies.**

Specify. Law Enforcement Agencies and their Attorney staff; State Child Support Agencies.

**Contractor** (Enter name and describe the language in the contract that safeguards PII.)

Specify. Willis Towers Watson

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

Specify. Private Attorneys, Authorized Third Party Individuals (i.e., spouse, dependents, employers, etc.), Financial Institutions

**G. Do individuals have the opportunity to object to the collection of their PII (opt-out)?**

Yes  No

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

Enrollment in benefits is a choice of the associate. Individuals are provided the Privacy Act Statement which includes the use and routine disclosures of the information they voluntarily provide to the Exchange. Individuals when appearing face-to-face with an Exchange associate have the option of withdrawing their desire to provide personal information. When information is requested through on-line environments or through forms, the individual has the authority to stop processing or completion of the form, choosing not to divulge their personal information. However, failure to provide information may affect the benefits provided to the individual.

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

n/a

**H. 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.

n/a

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

Information is used for proper processing of Benefits and pay associated with such elected benefits. Information provided is not used in a means for which it was not collected.

**I. What information is provided to an individual when asked to provide PII data? Indicate all that apply.**

Privacy Act Statement  Privacy Advisory  
 Exchange Privacy Policy  None

Other

Describe each applicable format listed above.

**AGENCY DISCLOSURE NOTICE**

The public reporting burden for this collection of information 0702-0139 is estimated to average 20 minutes per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding the burden estimate or burden reduction suggestions to the Department of Defense, Washington Headquarters Services, at [whs.mc-alex.esd.mbx.dd-dod-information-collections@mail.mil](mailto:whs.mc-alex.esd.mbx.dd-dod-information-collections@mail.mil). Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.

**PLEASE DO NOT RETURN YOUR RESPONSE TO THE ABOVE ADDRESS.**

Responses should be sent to your local AAFES HR Representative or to the AAFES HQ Treasury Benefit department at 3911 South Walton Walker Blvd., Dallas, TX 75236-1598.

**PRIVACY ACT STATEMENT**

**AUTHORITY:** Title 10 U.S.C. 7013, "Secretary of the Army"; Title 10 U.S.C. 9013, "Secretary of the Air Force"; Title 42 U.S.C. 659, "Consent by United States to income withholding, garnishment, and similar proceeding for enforcement of child support and alimony obligations"; 31 CFR 285.11, "Administrative Wage Garnishment"; DoD Directive 7000.14-R, Volume 13 and 16, "DoD Financial Management Regulation"; Department of Defense Instruction (DoDI) 1400.25, Volume 1408, "DoD Civilian Personnel Management System: Insurances and Annuities for Nonappropriated Fund (NAF) Employees"; Army Regulation 215-8/AFI 34-211(I), "Army and Air Force Exchange Service Operations"; and E.O. 9397 (SSN), as amended.

**PRINCIPAL PURPOSE(S):** Information collected is to provide the basis for computing civilian/retiree/survivor pay deductions and for processing of insurance benefits chosen by active Exchange associates.

**ROUTINE USE(S):** Your records may be disclosed outside of DoD pursuant to Title 5 U.S.C. §552a(b)(3) regarding DoD "Blanket Routine Uses" published at <http://dpcl.d.defense.gov/Privacy/SORNsIndex/BlanketRoutineUses.aspx>. Information may be disclosed to former spouses and/or survivors, to federal, state, or local child support agencies for purposes of assisting the agencies in the discharge of their responsibilities under federal and state law.

**DISCLOSURE:** Voluntary, however, failure to provide all the requested information may result in the denial of your application for benefits.

**SYSTEM OF RECORD NOTICE:** AAFES 0703.07 "Employee Pay System Records" available for view at <http://dpcl.d.defense.gov/Privacy/SORNsIndex>

**Website Privacy Notice**

LAST UPDATED: 4/10/2017

**THIS NOTICE DESCRIBES HOW PERSONAL INFORMATION ABOUT YOU MAY BE USED AND DISCLOSED AND HOW YOU CAN GET ACCESS TO THIS INFORMATION. PLEASE REVIEW IT CAREFULLY.**

Your current or former employer as the Plan Sponsor for the benefits you are eligible for has hired Willis Towers Watson to provide this website and other benefits administration services. Willis Towers Watson cares about your privacy and wants you to be familiar with how we collect, use, and disclose information. We use Personal Information to determine your benefit eligibility and validate any election information that is submitted through the application. This Privacy Notice describes our practices in connection with information that we collect through this website; telephone service center; employer data import files; other third-party import files approved by the Plan Sponsor; mobile devices; and HTML-formatted email messages that may be sent to you (collectively, the "Services"). By providing Personal Information to us, you agree to the terms and conditions of this Privacy Notice.

### Personal Information

"Personal Information" is information that identifies you as an individual or relates to an identifiable person, including, but not limited to:

- Name
- Address
- Social security number
- Birth date
- Gender
- Telephone number
- Email address
- Hire date, and dates of other changes in employment status
- Other information related to your benefit eligibility and election options

The information we collect is provided by the Plan Sponsor to confirm whether you, your spouse, and dependents are eligible for benefits. You may be asked to provide additional information about yourself, your spouse, your dependents, and beneficiary designations. You may also be asked to update or correct information about yourself, your spouse, or your dependents.

If you submit Personal Information relating to other people to us in connection with the Services, you represent that you have the authority to do so and to permit us to use the information in accordance with this Privacy Notice.

### How We May Collect Personal Information

We and our service providers may collect Personal Information in a variety of ways, including:

- Through the Sponsor of the Applicable Plans: We may collect Personal Information on encrypted, periodic, data transmission files from the Plan Sponsor. For most participants, the sponsor is your current or former employer.
- Through the Services: We may collect Personal Information through the Services; for example, when you process transactions through our online benefits portal.
- Offline: We may collect Personal Information from you offline, such as when you contact the service center.
- From Other Sources: We may receive your Personal Information from other sources, such as other third parties engaged by the Plan Sponsor to provide benefits-related services.

NOTE: A third party's use of information you provide to the third party shall be governed by the third party's privacy notice. Our use of information received from the third party shall be governed by this Privacy Notice.

### How We May Use Personal Information

We may use Personal Information:

- To respond to your inquiries and fulfill your requests, including to process the transactions you request such as enrolling you in the insurance carrier(s) you select.
- To generate your plan rates.
- To send administrative information to you.
- To track and record certain life status changes that enable you to make mid-year changes to your benefit elections.
- To provide you with related customer service.
- For our business purposes, such as data analysis, audits, developing new products, enhancing, improving or modifying our Services, identifying usage trends, and operating and expanding our business activities.
- As we believe to be necessary or appropriate: (a) under applicable law, including laws outside your country of residence; (b) to comply with legal process; (c) to respond to requests from public and government authorities, including public and government authorities outside your country of residence; (d) to enforce our terms and conditions; (e) to protect our operations or those of any of our affiliates; (f) to protect our rights, privacy, safety, or property, and/or that of our affiliates, including you; and (g) to allow us to pursue available remedies or limit the damages that we may sustain.
- For purposes of contacting you regarding the plan using an automated telephone dialing system and/or artificial or prerecorded voice.

### How Personal Information May Be Disclosed

Your Personal Information may be disclosed:

- To the Plan Sponsor (your employer): Limited information may be shared with the plan sponsor, including benefit elections; beneficiary information; and responses to questions to determine eligibility for certain benefits.

- To vendor partners selected by the Plan Sponsor to allow them to provide you with services associated with your benefits. Use of your Personal Information by vendor partners is governed by their privacy policies and not this Privacy Notice.
- To our third-party service providers who provide services such as website hosting, data analysis, payment processing, order fulfillment, information technology and related infrastructure, customer service, email delivery, and auditing.
- To anyone to whom you send messages through the Services, to allow the recipient to identify you.
- As we believe to be necessary or appropriate: (a) under applicable law, including laws outside your country of residence; (b) to comply with legal process; (c) to respond to requests from public and government authorities, including public and government authorities outside your country of residence; (d) to enforce our terms and conditions; (e) to protect our operations or those of any of our affiliates; (f) to protect our rights, privacy, safety or property, and/or that of our affiliates, including; and (g) to allow us to pursue available remedies or limit the damages that we may sustain.

#### OTHER INFORMATION

##### Other Information We May Collect

"Other Information" is any information that does not reveal your specific identity or does not directly relate to an individual, such as:

- Browser and device information
- App usage data
- Information collected through cookies and other technologies
- Demographic information and other information provided by you
- Aggregated information

If we are required to treat Other Information as Personal Information under applicable law, then we may use it for the purposes for which we use and disclose Personal Information as detailed in this Notice.

##### How We May Collect Other Information

We and our third-party service providers may collect Other Information in a variety of ways, including:

- Through your browser or device: Certain information is collected by most browsers or automatically through your device, such as your Media Access Control (MAC) address, computer type (Windows or Macintosh), screen resolution, operating system name and version, device manufacturer and model, language, Internet browser type and version, and the name and version of the Services you are using. We use this information to ensure that the Services function properly.
- Using cookies: Cookies are pieces of information stored directly on the computer that you are using. Cookies allow us to collect information such as browser type, time spent on the Services, pages visited, language preferences, and other anonymous traffic data. We and our service providers use the information for security purposes, to facilitate navigation, to display information more effectively, to personalize your experience while using the Services, and to recognize your computer in order to assist your use of the Services. We also gather statistical information about use of the Services in order to continually improve their design and functionality, understand how they are used, and assist us with resolving questions regarding them. If you disable cookies on the site, the site may not function properly.
- Analytics: We may use Google Analytics, which uses cookies and similar technologies to collect and analyze information about use of the Services and report on activities and trends. This service may also collect information regarding the use of other websites, apps and online resources. You can learn about Google's practices by going to [www.google.com/policies/privacy/?partners/](http://www.google.com/policies/privacy/?partners/), and opt out of them by downloading the Google Analytics opt-out browser add-on, available at <https://tools.google.com/dlpage/gaoptout>.
- IP Address: Your IP address is a number that is assigned to your computer by your Internet Service Provider (ISP). An IP address may automatically be identified and logged in our server log files whenever you, as a user, access the Services. This log may include the time and the page(s) visited. We use IP addresses to calculate usage levels, derive your approximate location, diagnose server problems, and administer the Services. We do not use IP addresses for identification or direct marketing purposes. Collecting IP addresses is a standard industry practice and is done automatically by many websites, applications, and other services.
- From you: Information such as your preferred means of communication is collected when



you voluntarily provide it.

- By aggregating information: Aggregated Personal Information does not personally identify you or any other user of the Services (for example, we may aggregate Personal Information to calculate the percentage of our users who have a particular telephone area code).

#### How We May Use and Disclose Other Information

We may use and disclose Other Information for any purpose, except as provided under applicable law. In some instances, we may combine Other Information with Personal Information. If we do, we will treat the combined information as Personal Information as long as it is combined.

If you have provided us with Personal Information, we may associate that information with the information about your usage of our site that is collected automatically.

#### THIRD-PARTY SERVICES

We may include links in the Services to websites for third parties, such as government agencies, carriers, and health and wellness providers. When you access these links, you will be leaving the Services and your usage of those third-party sites will be governed by the privacy policies of such third parties, not by this Privacy Notice. This Privacy Notice does not address, and we are not responsible for, the privacy, information, or other practices of any third parties, including any third party operating any site or service to which the Services may link. The inclusion of a link on the Services does not imply endorsement of the linked site or service, by us or by our affiliates.

#### SECURITY

We seek to use reasonable organizational, technical, and administrative measures to protect Personal Information within our organization. Unfortunately, no data transmission or storage system can be guaranteed to be 100% secure. If you have reason to believe that your interaction with us is no longer secure (for example, if you feel that the security of your account has been compromised), please immediately notify us in accordance with the "Contacting Us" section below.

#### CHOICES AND ACCESS

Your choices regarding our use and disclosure of your Personal Information

Our standard process is to send information regarding your benefits and other communications electronically via email or our online portal. You may request to receive communications by paper mail in accordance with the "Contacting Us" section below.

How you can access or change your Personal Information

If you would like to review, correct, or update Personal Information you may do so by contacting your Human Resources contact or accessing your employer's online benefits portal.

Please note that we may need to retain certain information for recordkeeping purposes and/or to complete any transactions that you began before you requested the change. There may also be residual information that will remain in our databases and other records, which will not be removed.

If you are a resident of California, under 18, and a registered user of the Services, you may ask us to remove content or information that you have posted to the Services in accordance with the "Contacting Us" section below. Please note that your request does not ensure complete or comprehensive removal of the content or information; for example, some of your content may have been reposted by another user.

#### RETENTION PERIOD

We will retain your Personal Information for the period necessary to fulfill the purposes outlined in this Privacy Notice, unless a longer retention period is required or permitted by law.

#### USE OF SERVICES BY MINORS

Because of the nature of our business, we do not solicit or intentionally receive information from children under the age of 13, except that we do collect information regarding dependent children that pertains to their benefits coverage and to beneficiary designations. Parents and legal guardians are permitted to provide us with information about their children.

#### CROSS-BORDER TRANSFER

Your Personal Information may be stored and processed in any country where we have facilities or in which we engage service providers. By using the Services you consent to the transfer of information to countries outside of your country of residence, including the United States, which may have data protection rules that are different from those of your country.

#### SENSITIVE INFORMATION

We ask that you not send us, and you not disclose, any sensitive Personal Information (for example, information related to racial or ethnic origin, political opinions, religion or other beliefs, health, biometrics or genetic characteristics, criminal background, or trade union membership) on or through the Services or otherwise to us.

#### UPDATES TO THIS PRIVACY NOTICE

We may change this Privacy Notice. The "Last Updated" legend at the top of this page indicates when this Privacy Notice was last revised. Any changes will become effective when we post the revised Privacy Notice. Your use of the Services following these changes means that you accept the revised Privacy Notice.

#### CONTACTING US

If you have any questions about this Privacy Notice or how your Personal Information may be used or disclosed, please contact us at [privacy@willistowerswatson.com](mailto:privacy@willistowerswatson.com), or call toll-free at 888-471-4502.

Because email communications are not always secure, please do not include credit card or other sensitive information in your emails to us.

For all other inquiries, refer to the Contact Us information available on this website or customer service contact information provided by your Plan Sponsor.

#### **NOTE:**

**Sections 1 and 2 above will be posted to the Exchange's Web site. Posting of these Sections indicates that the PIA has been reviewed to ensure that appropriate safeguards are in place to protect privacy.**

**The Exchange may restrict the publication of Sections 1 and/or 2 if they contain information that would reveal sensitive information or raise security concerns.**