

**PRIVACY IMPACT ASSESSMENT (PIA)**

For the

Customer Care Center Enterprise Solution

Defense Finance and Accounting Service

**SECTION 1: IS A PIA REQUIRED?**

a. Will this Department of Defense (DoD) information system or electronic collection of information (referred to as an "electronic collection" for the purpose of this form) collect, maintain, use, and/or disseminate PII about members of the public, Federal personnel, contractors or foreign nationals employed at U.S. military facilities internationally? Choose one option from the choices below. (Choose (3) for foreign nationals).

- (1) Yes, from members of the general public.
- (2) Yes, from Federal personnel\* and/or Federal contractors.
- (3) Yes, from both members of the general public and Federal personnel and/or Federal contractors.
- (4) No

\* "Federal personnel" are referred to in the DoD IT Portfolio Repository (DITPR) as "Federal employees."

b. If "No," ensure that DITPR or the authoritative database that updates DITPR is annotated for the reason(s) why a PIA is not required. If the DoD information system or electronic collection is not in DITPR, ensure that the reason(s) are recorded in appropriate documentation.

c. If "Yes," then a PIA is required. Proceed to Section 2.

**SECTION 2: PIA SUMMARY INFORMATION**

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

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

**b. Is this DoD information system registered in the DITPR or the DoD Secret Internet Protocol Router Network (SIPRNET) IT Registry?**

- Yes, DITPR      Enter DITPR System Identification Number
- Yes, SIPRNET      Enter SIPRNET Identification Number
- No

**c. Does this DoD information system have an IT investment Unique Project Identifier (UPI), required by section 53 of Office of Management and Budget (OMB) Circular A-11?**

- Yes
- No

If "Yes," enter UPI

If unsure, consult the Component IT Budget Point of Contact to obtain the UPI.

**d. Does this DoD information system or electronic collection require a Privacy Act System of Records Notice (SORN)?**

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

If "Yes," enter Privacy Act SORN Identifier

DoD Component-assigned designator, not the Federal Register number.  
Consult the Component Privacy Office for additional information or  
access DoD Privacy Act SORNs at: <http://www.defenselink.mil/privacy/notices/>

or

**Date of submission for approval to Defense Privacy Office**  
Consult the Component Privacy Office for this date.

**e. Does this DoD information system or electronic collection have an OMB Control Number?**  
Contact the Component Information Management Control Officer or DoD Clearance Officer for this information.

This number indicates OMB approval to collect data from 10 or more members of the public in a 12-month period regardless of form or format.

**Yes**

**Enter OMB Control Number**

Submitted for approval on March 15, 2013

**Enter Expiration Date**

**No**

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

(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 DoD information system or electronic collection to collect, use, maintain and/or disseminate PII. (If multiple authorities are cited, provide all that apply.)

(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) DoD Components can use their general statutory grants of authority ("internal housekeeping") as the primary authority. The requirement, directive, or instruction implementing the statute within the DoD Component should be identified.

**AUTHORITY FOR MAINTENANCE OF THE SYSTEM:**

5 U.S.C. 301, Departmental Regulations; E.O. 12862 (Customer Service), E.O. 9397 (SSN) as amended.

**ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING CATEGORIES OF USERS AND THE PURPOSES OF SUCH USES:**

In addition to those disclosures generally permitted under 5 U.S.C. 552a(b) of the Privacy Act, these records or information contained therein may specifically be disclosed outside the DoD as a routine use pursuant to 5 U.S.C. 552a(b)(3) as follows:

The 'DoD Blanket Routine Uses' published at the beginning of the DFAS compilation of systems of records notices apply to this system.

**g. Summary of DoD 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 DoD information system or electronic collection and briefly describe the types of personal information about individuals collected in the system.

This Customer Care Center Enterprise Solution (CCCES) is made up of the following components and provides DFAS with a solution that will create operational efficiencies, lower cost, improve customer service quality, and reduce agency audit risk:

- a. Agent Platform – Component responsible for delivering voice communications via a scalable and flexible set of tools and applications. It is the means by which customer inquiries will be delivered to the CSR for resolution. This platform will support the inquiry routing and distribution to the CSRs, the IVR, self-service, wait-in-queue outbound dialing, workforce management, call recording, metric gathering, and analysis.
- b. Customer Relationship Management (CRM) – Component that creates a 360-degree view of customer data, which will allow CSRs to help their customers quicker by reducing the number of screen pops and sign-on requirements based on an intuitive, rules-based business engine and data integration of DFAS systems
- c. Knowledge Base (KB) – Component that integrates frequently asked questions (FAQs) and business processes that are accessible to CSRs and provides benefits that include faster training, more consistent and accurate answers, and the ability to share workload between and among different CCC agent groups and sites

The CCCES will collect all data necessary in order to service DFAS Customer Inquiries, this includes all of the information that is checked in Section 3 of this PIA.

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

The result of mishandling personal data may lead to lost, stolen or compromised PII which could be harmful to the individual in many ways (e.g., identify theft, damage to the individual's reputation and /or financial hardship). Such incidents could cast DFAS in an unfavorable light to the public. Hence, access to the CCCES is limited to persons authorized to use the system in performance of their official duties (requires screening and documented approval utilizing DD Form 2875). User access to the system will be via DoD CAC authentication. The system adheres to physical protections of PII as described in accordance with DFAS 5200.1-R. IA policy (DFAS 8400.1-R) prescribes protection requirements for sensitive data, to include PII, for all DFAS systems. Management responsibilities for protecting data are maintained in DFAS 8500.1. The CCCES will inherit many of the defense in depth mechanisms already in place on the DFAS Enterprise Local Area Network (ELAN). This includes:

- a. Network perimeter protection: Firewalls filter WAN traffic through configured policies and Access Control Lists (ACL), and the network IPS filters unauthorized traffic. Firewall ports, protocols, and services have been verified and validated against the DoD Ports, Protocols, and Services Assurance Category List, published under the authority of DoD 8551.1, Ports, Protocols, and Services Management.
- b. Authentication: Public Key Infrastructure (PKI) infrastructure is required for all DFAS users, to include CCCES CSR personnel and system administrators for authentication. This utilizes security attributes of Common Access Card (CAC) authentication and digital certificates and is integrated with the ELAN Active Directory (AD) Infrastructure.
- c. Virus protection: McAfee Antivirus products as offered by the required Host Based Security System (HBSS) provide automated virus and spyware protection for compatible CCCES systems. This protection is required per Operations Order (OPORD) 12-1016 that supports USCYBERCOM OPOrd 11-02 Operation Gladiator Shield (OGS) requirements.
- d. Host Protection: In addition to Virus Protection, HBSS point products are deployed throughout the DFAS CCCES, as compatible. Point Products include: Host Intrusion Prevention System, Policy Auditor, Asset Configuration Control Module, and Asset Baseline Monitor.
- e. System Hardening: All Operating Systems and associated backend databases that are within the ELAN accreditation boundary are built utilizing DISA Security Technical Implementation Guides (STIGs) and standard ELAN Platform and Engineering Team hardened images, installation and configuration documentation. Joint Interoperability Test Center (JITC) has certified the DFAS CCCES telephony architecture.

Additionally, communications between CCCES and interconnected systems outside the DFAS enclave are achieved through either a Site-to-Site encrypted Internet Protocol Security (IPsec) tunnel as part of the VPN connection grid

or thru Point-to-Point secure communication protocols.

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

**Within the DoD Component.**

Specify. PII Information will be retrieved from multiple interconnected DoD systems, however the information received will not be electronically exchanged between any systems residing outside of the DFAS enclave.

**Other DoD Components.**

Specify.

**Other Federal Agencies.**

Specify.

**State and Local Agencies.**

Specify.

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

Specify.

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

Specify.

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

**Yes**  **No**

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

Individual may choose not to provide PII voluntarily. The individual also has the option to speak to a service desk agent without entering their PII data. However, failure to furnish the requested information will result in the individual's request not being properly serviced as without the PII, authentication and verification cannot be conducted, which results in no authorization to provide service on individual account details.

(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.

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

Users data is collected in order to service the callers needs; however, there is currently no verbal advisory as to the specific uses of the data provided. Once a call is connected to an agent and the caller has not provided any PII, the caller has the option of authenticating with verbal submission of PII to the agent. However, the agent does not present that caller with a verbal Privacy Act Statement to obtain consent of use specific uses.

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

- |  |   |
|--|---|
| <input type="checkbox"/> Privacy Act Statement | <input type="checkbox"/> Privacy Advisory |
| <input type="checkbox"/> Other                 | <input checked="" type="checkbox"/> None  |

Describe each applicable format.

--

**NOTE:**

**Sections 1 and 2 above are to be posted to the Component'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.**

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