PRIVACY IMPACT ASSESSMENT (PIA)

For the

Air Combat Command (ACC) Collaborative Environment (ACE)
United States Air Force - Air Combat Command

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: 11854
- ☐ **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

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.

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.

The purpose of the ACC Collaborative Environment (ACE) is to provide increased availability and accessibility of information, facilitate cross-functional project collaboration and communication capabilities for warfighter and combat support mission execution. ACC Collaborative Environment (ACE) is comprised of Microsoft Office SharePoint Server (MOSS), Microsoft Office Communications Server (OCS), Microsoft Dynamics Customer Relationship Management and IBM FileNet P8 software. ACE will provide integrated intranet portals, team workspaces, integrated e-mail, presence awareness, instant messaging, web-based video/audio conferencing and task management. These integrated technologies create a complete portfolio of collaboration and communication services to connect people, organizations, information and processes across geographic boundaries. The ACC Collaborative Environment (ACE) implementation will solve key organizational computing challenges such as: finding up-to-date information/documentation, quickly increasing team and project productivity, connecting people and organizations more efficiently, providing a common planning and management environment, and providing ease of use by all users with varying levels of computer skills. MOSS facilitates a common framework and communication channel across all of the applications within The The purpose of the ACC Collaborative Environment (ACE) is to provide increased availability and accessibility of information, facilitate cross-functional project collaboration and communication capabilities for war fighter and combat support mission execution. This allows ACC Collaborative Environment (ACE) to serve not only as a collaborative environment, but also as a development platform on which new customized applications, web parts and portals can easily be created to meet new mission requirements without deploying new systems. Initiatives developed within ACC Collaborative Environment (ACE) inherit core security controls from Active Directory (AD) via the Microsoft .Net framework. An example of this is the Evaluation Management System (EMS), which is a workflow application designed within ACC Collaborative Environment (ACE) to facilitate and standardize the routing/coordination of Officer and Enlisted Evaluations and Awards/Decorations with role-based permissions access on a need-to-know basis. Users are authenticated by the Active Directory (AD) within MOSS and are only able to access documents, folders or other items based on need-to-know. Many of the current custom ACC Collaborative Environment (ACE) applications focus on biographical, task and records management data. However, future development initiatives may collect or store other forms of Personally Identifiable Information (PII). Information is never released to the public.

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

The risk associated with storing Personally Identifiable Information (PII) within ACC Collaborative Environment (ACE) is that individuals could be identified based on the data, documents or other information stored within slected file folders. In order to mitigate these risks, site administrators, owners and users are provided Privacy Act training. All folders containing PII elements will follow DoD 5400.11, AFI 33-332, and AFI 33-129 guidance for the maintenance of PII data. Folder access will be limited to those individuals with a need-to-know in order to perform their job. Folder access will be limited to those individuals with a need to know in order to perform their jobs. Software architects involved in the development of ACC Collaborative Environment (ACE) applications, portals or web parts will assess all development initiatives for privacy impact. Software architects will coordinate with the Privacy Act office prior to beginning any new design project. This will ensure all mitigating risks will be reviewed and all required changes will be incorporated to include the display of appropriate privacy disclosure statements as required.

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. Headquarter Air Combat Command and Wings

☐ **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.

Much of the Personally Identifiable Information (PII) collected and stored within ACE is inherited from Active Directory (AD), while other PII may be collected from users via custom forms. Biographies collected on users My Site contain information the individuals provide themselves. Some Personally Identifiable Information (PII) is provided directly for other privacy act systems of record. For example, the Officer/ Enlisted Evaluation forms routed through the Evaluation Management System (EMS) application are generated through the Personnel System at Randolph Air Force Base.

(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.

Biographical information collected on My Site is input into the system directly by the individuals themselves. Some Personally Identifiable Information (PII) is provided directly for other privacy act systems of record. For example, the Officer/Enlisted Evaluation forms routed through the Evaluation Management System (EMS) application are generated through the Personnel System at Randolph Air Force Base.

(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.

☒ **Privacy Act Statement** ☐ **Privacy Advisory**

☒ **Other** ☐ **None**

Describe each applicable format.

An appropriate Privacy Act statement is provided (as referenced in AFI 33-332) when users are requested to provide personally identifiable information (PII) and individuals have the choice whether to enter this information or not. Example alert statements for the My Site section of SharePoint include: "Use this document library for documents that you want to keep for personal use. They will only be visible to you and administrators for the server." and "Use this document library to store your documents. Documents shared here will be displayed on your public home page." Locked file folders containing Evaluation Management System (EMS) evaluation documents contain the following Privacy Act warning label on each individual folder being routed through the system:

"This document contains FOR OFFICIAL USE ONLY (FOUO)
information which must be protected under the Privacy Act and AFI 33-332."

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.

SECTION 3: PIA QUESTIONNAIRE and RISK REVIEW

a. For the questions in subparagraphs 3.a.(1) through 3.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 below.

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

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

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

Information is provided directly from the individual or from other approved Privacy Act systems of record. MilPDS (EPR/OPR Notices, DECOR6), ARMS/PRAD (e-UPRG) and AFFMS (AF Fitness Mgmt System) for current PT results will be obtained from the supporting Information System.

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

☐	**Paper Form**	☐	**Face-to-Face Contact**
☐	**Telephone Interview**	☐	**Fax**
☒	**Email**	☒	**Web Site**
☒	**Information Sharing - System to System**		
☒	**Other**		

Working and supporting documents are uploaded and/or created in the ACC Collaborative Environment (ACE).

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

The purpose of the ACC Collaborative Environment (ACE) is to provide increased availability and accessibility of information, facilitate cross-functional project collaboration and communication capabilities for the war fighter and combat support mission execution. ACE will provide integrated intranet portals, team work spaces, integrated e-mail, presence awareness, instant messaging, web-based video/audio conferencing and task management. These integrated technologies create a complete portfolio of collaboration and communication services to connect people, organizations, information and processes across geographic boundaries. The ACE implementation will solve key organizational computing challenges such as: finding up-to-date information/documentation, quickly increasing team and project productivity, connecting people and organizations more efficiently, providing a common planning and management environment, and providing ease of use by all users with varying levels of computer skills. For example, the Evaluation Management System's supporting documentation is provided as prescribed by AFI 36-2803 (AF Awards & Decorations Program) as justification for the recommendation. AFI 36-2406 (Officer & Enlisted Evaluation System), including AFPC published MPFMs and PSDMs.

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

The information stored in ACC Collaborative Environment (ACE) is intended to support the administrative needs of Air Combat Command in meeting its mission goals.

b. Does this DoD 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 this DoD information system or electronic collection? Indicate all that apply.

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

☐ **Other**

Biographies collected on each users' MySite will contain information which has been provided by the individuals themselves and is available to all ACE users. Other forms of PII, collected from other privacy act systems of record or custom forms, will be restricted on a need to know basis. Developers or contractors hired to perform development tasks will have limited access to PII data only to test the design capabilities of the applications, web parts or portals being designed.

d. How will the PII be secured?

(1) Physical controls. Indicate all that apply.

☒	**Security Guards**	☒	**Cipher Locks**
☒	**Identification Badges**	☐	**Combination Locks**
☒	**Key Cards**	☒	**Closed Circuit TV (CCTV)**
☐	**Safes**	☒	**Other**

Physical access to ACC Collaborative Environment (ACE) servers and backups is strictly controlled and limited by the AFSPC 83rd NOS and ACC 82nd Communications Group. Role-based permissions are applied to all folders containing PII data.

(2) Technical Controls. Indicate all that apply.

☒	**User Identification**	☐	**Biometrics**
☒	**Password**	☒	**Firewall**
☒	**Intrusion Detection System (IDS)**	☐	**Virtual Private Network (VPN)**
☒	**Encryption**	☒	**DoD Public Key Infrastructure Certificates**
☐	**External Certificate Authority (CA) Certificate**	☒	**Common Access Card (CAC)**
☐	**Other**		

ACC Collaborative Environment (ACE) inherits its core security from Active Directory (AD). System architects develop application, web parts or portals within the ACC Collaborative Environment (ACE) utilizing Active Directory (AD) authentication via the Microsoft.net framework. Administrators and

information owners can modify permissions based on a need to know basis. The system inherits IDS, firewall, encryption and certificates from core services provided by the AF GIG.

(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**

☐ **Other**

e. Does this DoD information system require certification and accreditation under the DoD Information Assurance Certification and Accreditation Process (DIACAP)?

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

☐	**Authorization to Operate (ATO)**	**Date Granted:**	
☒	**Interim Authorization to Operate (IATO)**	**Date Granted:**	15 Jan 2010
☐	**Denial of Authorization to Operate (DATO)**	**Date Granted:**	
☐	**Interim Authorization to Test (IATT)**	**Date Granted:**	

☐ **No, this DoD information system does not require certification and accreditation.**

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?

Documents contained in SharePoint are for collaboration only; documents are removed when finalized. Access to documents containing PII elements is limited on a need to know basis.

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

The ACC Portfolio Manager (PM) notifies the ACC Privacy Act manager when a new system is identified in EITDR; the Privacy Act manager provides training for the new program manager immediately within 30 days of notification. Within this 30 days the Privacy Act manager meets with the program manager and reviews the system to assess the privacy risks involved and determine what action is required. The ACC 82nd Communications Squadron notifies the Privacy Act office whenever a new design request is received and the Privacy Act manager meets with both the program manager and the design team to assess risks and determine a plan of action. Privacy Act training is included with the SharePoint site owners training. Site owners are required to review information on a regular basis and report any PII violates to the ACC or appropriate Wing Privacy Act manager.

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

N/A