PRIVACY IMPACT ASSESSMENT (PIA)

For the

Leadership Mirror 360
United States Air Force

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: 1015295
- ☐ **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.

28 August 2009

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.

10 United States Code (USC) 8013, Secretary of the Air Force; Air Force Instruction 33-213, Identity Management

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 application is hosted by a contractor in Pittsburgh, PA and uses a commercial [.net] web-based access link to allow an invited user to conduct a 360 degree assessment that is designed to collect perception-based feedback for individuals based on Air Force institutional competencies. It is used to support Force Development (FD) needs of USAF personnel and is administered out of Headquarters Air Force, Directorate of Force Development, HAF/A1D. USAF administrators launch e-mail notifications to the appropriately identified USAF personnel, asking them to complete their self-assessment and select others as raters to complete an assessment on their behalf. PII data derived from data already maintained by AF/A1 is utilized to appropriately identify those individuals being asked to complete a LM 360 survey. The types of PII involved are: First name, last name, middle name (when available), e-mail address, rank, Major Command (MAJCOM), Air Force Speciality Code (AFSC) and/or Occupational Series, and Electronic Data Interchange-Personal Identifier (EDI-PI).

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

PII collected is only accessible by USAF personnel (civilian, military, or contractor) that are completing a LM 360 assessment in conjunction with the performance of the official duties. The PII represents the same access of information and/or data elements made available to USAF personnel via the Air Force Global Address List (AF GAL). Users of the LM 360 application have to be granted access by a designated LM 360 administrator who are in turn designated by HAF/A1D. PII access is achieved by accessing a .com site via assigned password and user name using Hyper Text Transport Protocol in a Secure Sockets Layer encrypted session (HTTPS) using approved Department of Defense (DoD) Encryption methodologies.

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. Air Force Directorate of Force Management

☐ **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. Development Dimensions International (DDI), AF Contractor for LM 360 - PII is safeguarded via assigned user password and user name using Hyper Text Transport Protocol in a Secure Sockets Layer encrypted session (HTTPS) using approved Department of Defense (DoD) Encryption methodologies in addition to physical

security measures for servers.

☐ **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.

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

LM 360 does not collect PII. PII data is contained and derived from data already maintained from AF/A1. All data collected by AF/A1 is in compliance with agreed upon USAF and owning organizations' Memorandums of Agreement (MOAs) and Interface requirements documents. All data related to Leadership Mirror for PII is transferred via Secure LDAP and HTTPS using DoD encryption methodologies. Due to the nature of the data transfer, the information is not in an identifiable form. In compliance with AFI 33-332, Privacy Act Program, paragraph 12.4.1, any data released without consent of the subject are requested in the performance of official duties.

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.

PII data is contained and derived from data already maintained from AF/A1. All data collected by AF/A1 is in compliance with agreed upon USAF and owning organizations' Memorandums of Agreement (MOAs) and Interface requirements documents. All data related to Leadership Mirror for PII is transferred via Secure LDAP and HTTPS using DoD encryption methodologies. Due to the nature of the data transfer, the information is not in an identifiable form. In compliance with AFI 33-332, Privacy Act Program, paragraph 12.4.1, any data released without consent of the subject are requested in the performance of official duties.

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.	Individuals are not asked to provide PII data as it is contained and derived from data already maintained by AF/A1.

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.