PRIVACY IMPACT ASSESSMENT (PIA)

For the

Emergency Mass Notification System
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	8960
☐	**Yes, SIPRNET**	Enter SIPRNET Identification Number	N/A
☐	**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 007-57-02-45-01-2818-00

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 F010 AFSPC A

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.

Air Force Policy Directive 10-2 Readiness, Air Force Policy Directive 10-4 Operations Planning, and Air Force Policy Directive 10-25 Emergency Management, Air Force Instruction 10-207 Command Posts, and Air Force Instruction 10-218 Personnel Accountability in Conjunction with Natural Disasters or National Emergencies.

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 system serves as part of the Air Combat Command Emergency Mass Notification System and it provides rapid notification of time-critical/time sensitive alerts to the chain of command as well as disseminates urgent information to the base populace in a timely manner. It has the capability to notify members in the Emergency Mass Notification System database, via electronic or telephone devices, of personnel recalls, real-world and exercise threat conditions, and of natural or man-made disasters. Notifications can also be made via the Installation Notification and Warning System, aka Giant Voice. The system vendor is AtHoc, the system owner is Air Combat Command Command and Control Systems at Langley Air Force Base, VA, and will be operated by the Air Combat Command Command Center and Installation Command Posts. Similar systems exist within Air Force Reserve Command, Air Education Training Command, and Air Mobility Command. Type of personal information gathered will be for notification purposes only and will aid the Installation Command Post in making immediate notifications to base populace. The backup for this system is the paper hardcopy of the recall rosters.

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

Information collected will be the individual's first and last name, rank/title, military status, office symbol, duty building number, base location, duty phone, duty electronic mail address, home zip code, home phone, cell phone, home electronic mail address, and Short Message Service text address. All Personally Identifiable Information reports generated from Emergency Mass Notification System will be used for the sole purpose of confirming receipt of alert messages. These reports will only be reviewed by Command Post personnel and applicable leadership authorities and then will be shredded upon completion of need. Access to the Emergency Mass Notification System is located via the Base Local Area Network where access is limited to valid Common Access Card users. Emergency Mass Notification System users, as designated by the Installation Command Post, are further restricted by an Emergency Mass Notification System user identification and password.

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. Personally Identifiable Information as outlined above will only be shared with DoD Leadership with a valid 'need-to-know' requirement in regard to recalling specific military and key Air Force civilian personnel in support of national defense and security policy.

☐ **Other DoD Components.**

Specify. N/A

☐ **Other Federal Agencies.**

Specify. N/A

☐ **State and Local Agencies.**

Specify. N/A

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

Specify. N/A

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

Specify. N/A

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.

Non-key civilians may elect to object to the collection of this Personally Identifiable Information. This is identified in the web-based Self Service page where this information is entered by each individual. Objection can be easily accomplished by simply not inputting their personal information into the system. When this information is requested by individuals, a Privacy Act Statement is provided which informs them that the collection is not mandatory for non-key civilians. Military members and key civilians do not have the option to object to the collection of duty related elements but they are not required to input the remaining Personally Identifiable Information. Mandatory information is office symbol, base, base zip code, and duty building number. All other information is optional for these individuals. Authority: Air Force Policy Directive 10-2 Readiness, Air Force Policy Directive 10-4 Operations Planning, Air Force Policy Directive 10-25 Emergency Management, Air Force Instruction 10-207 Command Posts, and Air Force Instruction 10-218 Personnel Accountability in Conjunction with Natural Disasters or National Emergencies.

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

N/A

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 act of inputting the Personally Identifiable Information into Emergency Mass Notification System constitutes the consent for specific use. The instructions given to individuals upon account creation states that by inputting their information in this system, they are giving their consent for its use as stated in the Privacy Act Statement. This is identified in the web-based Self Service page where this information is inputted by each individual. Objection can be easily accomplished by simply not inputting their home telephone information, cell phone, or personal home email address in the system. When this information is requested by individuals, a Privacy Act Statement is provided which informs them that the collection is voluntary not mandatory for non key-civilians but mandatory for Military members and key-civilians. Authority: Air Force Policy Directive 10-2 Readiness, Air Force Policy Directive 10-4 Operations Planning, Air Force Policy Directive 10-25 Emergency Management, Air Force Instruction 10-207 Command Posts, and Air Force Instruction 10-218 Personnel Accountability in Conjunction with Natural Disasters or National Emergencies.

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

N/A

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.	AUTHORITY: Air Force Policy Directive 10-2, Air Force Policy Directive 10-4, Air Force Policy Directive 10-25, Air Force Instruction 10-207, and Air Force Instruction 10-218. PURPOSE: ACC EMNS satisfies the Installation Notification and Warning System requirements by providing the capability to deliver commander directed notifications and alerts. With this system, notification methods can be delivered via desktop pop-up messages, electronic mail, telephone, and Giant Voice devices regardless of time of day. All personal information gathered will only be used within the Air Force chain of command to determine the status of alerts received by targeted recipients. Additionally, if a report is printed to document this confirmation, the list will be protected FOR OFFICIAL USE ONLY and shredded when no longer required. ROUTINE USES: Information gathered will not be released outside DoD channels. DISCLOSURE: Disclosure is mandatory for military and key civilians and voluntary for non-key civilians. Failure to disclose information would result in not being notified of mission-essential or emergency information.

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.