PRIVACY IMPACT ASSESSMENT (PIA)

PRESCRIBING AUTHORITY: DoD Instruction 5400.16, "DoD Privacy Impact Assessment (PIA) Guidance". Complete this form for Department of Defense (DoD) information systems or electronic collections of information (referred to as an "electronic collection" for the purpose of this form) that collect, maintain, use, and/or disseminate personally identifiable information (PII) about members of the public, Federal employees, contractors, or foreign nationals employed at U.S. military facilities internationally. In the case where no PII is collected, the PIA will serve as a conclusive determination that privacy requirements do not apply to system.

1. DOD INFORMATION SYSTEM/ELECTRONIC COLLECTION NAME:

ALERT - ALERT! TELEPHONE AND NETWORK ALERTING SYSTEM

2. DOD COMPONENT NAME:

United States Army

3. PIA APPROVAL DATE:

08/25/20

HQDA DAMO-AP, G34

SECTION 1: PII DESCRIPTION SUMMARY (FOR PUBLIC RELEASE)

a. The PII is: *(Check one. Note: foreign nationals are included in general public.)*

- [ ] From members of the general public
- [x] From Federal employees and/or Federal contractors
- [ ] From both members of the general public and Federal employees and/or Federal contractors
- [ ] Not Collected *(if checked proceed to Section 4)*

b. The PII is in a: *(Check one)*

- [ ] New DoD Information System
- [ ] New Electronic Collection
- [x] Existing DoD Information System
- [ ] Existing Electronic Collection
- [ ] Significantly Modified DoD Information System

c. Describe the purpose of this DoD information system or electronic collection and describe the types of personal information about individuals collected in the system.

Per DoD Instruction 6055.17, all DoD Installations shall maintain mass warning and notification capabilities to warn all personnel immediately, but no longer than 10 minutes after incident notification and verification.

Secretary of Defense MFD : Force Protection Efforts OSD010319-15/CMD013583-15: Requirement to install additional mass warning and alert notifications to help safeguard DoD personnel.

Alert! is a Government Off The Shelf (GOTS) based network-centric emergency mass notification syst==sktop alerts, phone, SMS text messages, email, Giant Voice and Indoor Voice. In order to accurately notify registered users, the Alert! system must collect work and personal contact information to perform phone, SMS text and email notifications.

The Alert! system architecture consists of web applications, database servers, desktop client software, and interfaces to third-party phone/ SMS service providers. Users are registered in the Alert! system either by manual input from an assigned registrar on a web-based registration form or by manual input from a mandatory registration form on the desktop client software. Once registered, the user has the option of updating their information via the desktop client software or submitting updates to an assigned registrar or system administrator.

PII collected includes: name (first, middle, last), rank, Comman Access Card (CAC) Common Name (CN), organization, command, subcommand, work and home phone numbers, work and home email addresses, work and home physical addresses. Not all fields are required. The following fields are mandatory on the user registration form:

First Name
Last Name
Rank
CAC CN
1 or more work or home phone number
1 or more work or home email address

For phone number and email address inputs, the user has the option of opting out of providing this information but must provide a reason for opting out.

The following fields are optional on the user registration form:
Middle Name
Organization

Command
Subcommand
1 or more work or home addresses

d. Why is the PII collected and/or what is the intended use of the PII? *(e.g., verification, identification, authentication, data matching, mission-related use, administrative use)*

CAC common name is used for identification and verification of users and authentication of system operators and system administrators to the Alert! web interface.

Phone number and email address data is used for sending alert notifications via automated phone call, SMS text messages and email.

Address data is used for geocoding the physical location of the user. The calculated physical location (typically GPS location data) is used in conjunction with the geospatial bounding area of an alert to determine if the registered user should be notified.

The intended use of collected PII is mission-related. PII information is strictly used to allow system access to the Alert! web applications (CAC CN) and to communicate alert notifications to registered users via phone, SMS text message and/or email.

e. Do individuals have the opportunity to object to the collection of their PII? ☐ Yes ☒ No

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

(2) If "No," state the reason why individuals cannot object to the collection of PII.

No, in accordence with DoDi 6055.17 Section 5.5 MWN. Due to the life-safety implications of the information being relayed and the requirement to provide immediate alerts and warnings, members of the primary population must ensure their personal contact information, including after-duty hours contact information (e.g., personal cellular phone numbers and/or landlines phone numbers), e-mail addresses, home address, etc., are entered into the system and regularly updated or verified every 90 days to remain current and accurate.

f. 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.

The phone number and email address fields on the user registration form are mandatory but allow the user to opt-out of filling out these fields. In addition, the phone number includes an optional "Receive SMS" checkbox that allows the user to opt-in to receive SMS text messages. By default, providing a phone number will only support receiving phone notifications.

g. When an individual is asked to provide PII, a Privacy Act Statement (PAS) and/or a Privacy Advisory must be provided. *(Check as appropriate and provide the actual wording.)*

☒ Privacy Act Statement ☐ Privacy Advisory ☐ Not Applicable

Privacy Act Statement is displayed via link on Alert! Web Interface site and is accessible after the user authenticates with the web application.

Privacy Act Statement

AUTHORITY: 5 U.S.C. Section 301; 10 U.S.C. chapter 147; 10 U.S.C. Sections 1061 - 1065, 1072 - 1074, 1074a - 1074c, 1074c(1), 1076, 1076a, 1077, 1095(k)(2); 50 U.S.C. chapter 23; E.O. 9397; E.O. 10450, as amended.

PURPOSE: To receive emergency mass notification warnings from an automated system. The alerts will provide timely warning of potentially life-threatening scenarios, such as acts of terror, violence, extreme weather, or other catastrophic events.

ROUTINE USES: Most Emergency Services personnel will have access to send out notifications to the means of communication specified during registration. This could potentially include phone calls and SMS to personal mobile and home phones, as specified by the registrant during the registration process. This information is not routinely shared with other Information within the DOD or Federal Government. Phone Numbers are sent to a third party commercial telephony services provider. However, names and all other PII are excluded from the data sent to those providers. Responses to the alert are recorded. Additionally, all attempts to contact and their disposition - including any responses, are recorded.

DISCLOSURE: Disclosure of personal contact information is voluntary. However, failure to provide adequate personal contact information could delay notification of potentially life-threatening scenarios.

h. With whom will the PII be shared through data exchange, both within your DoD Component and outside your Component? *(Check all that apply)*

☒ Within the DoD Component Specify. EOC, US ARMY, US NAVY, DISA, US AIR FORCE, US MARINES

☐ Other DoD Components	Specify.	
☐ Other Federal Agencies	Specify.	
☐ State and Local Agencies	Specify.	
☐ Contractor *(Name of contractor and describe the language in the contract that safeguards PII. Include whether FAR privacy clauses, i.e., 52.224-1, Privacy Act Notification, 52.224-2, Privacy Act, and FAR 39.105 are included in the contract.)*	Specify.	
☐ Other *(e.g., commercial providers, colleges).*	Specify.	

i. Source of the PII collected is: *(Check all that apply and list all information systems if applicable)*

- ☒ Individuals
- ☐ Existing DoD Information Systems
- ☐ Other Federal Information Systems
- ☒ Databases
- ☐ Commercial Systems

PII data is input into the Alert! system in 3 ways:

The first method is by the individual via the user registration form on the desktop alert client software.

The second method is by system administrators and registrars (operators) entering PII for individuals via a web-based user registration form.

The third method is via system to system synchronization with data replication across COOP and primary site exchange over secure network Ports Protocols and Services.

j. How will the information be collected? *(Check all that apply and list all Official Form Numbers if applicable)*

- ☐ E-mail
- ☐ Face-to-Face Contact
- ☐ Fax
- ☒ Information Sharing - System to System
- ☐ Other *(If Other, enter the information in the box below)*
- ☐ Official Form (*Enter Form Number(s) in the box below)*
- ☐ Paper
- ☐ Telephone Interview
- ☒ Website/E-Form

k. 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 must be consistent.

☒ Yes ☐ No

If "Yes," enter SORN System Identifier DCIO 02 DoD

SORN Identifier, not the Federal Register (FR) Citation. Consult the DoD Component Privacy Office for additional information or http://dpcld.defense.gov/Privacy/SORNs/

or

If a SORN has not yet been published in the Federal Register, enter date of submission for approval to Defense Privacy, Civil Liberties, and Transparency Division (DPCLTD). Consult the DoD Component Privacy Office for this date

If "No," explain why the SORN is not required in accordance with DoD Regulation 5400.11-R: Department of Defense Privacy Program.

l. What is the National Archives and Records Administration (NARA) approved, pending or general records schedule (GRS) disposition authority for the system or for the records maintained in the system?

(1) NARA Job Number or General Records Schedule Authority. GRS 5.3, item 020 (DAA-GRS-2016-0004-0002)

(2) If pending, provide the date the SF-115 was submitted to NARA.

(3) Retention Instructions.

500-3d, KEN. Event is when superseded or obsolete. Keep in CFA until event occurs and then until no longer needed for conducting business, but not longer than 6 years after the event, then destroy.

m. What is the authority to collect information? A Federal law or Executive Order must authorize the collection and maintenance of a system of records. For PII not collected or maintained in a system of records, the collection or maintenance of the PII must be necessary to discharge the requirements of a statue or Executive Order.

(1) If this system has a Privacy Act SORN, the authorities in this PIA and the existing Privacy Act SORN should be similar.
(2) If a SORN does not apply, 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) Cite the specific provisions of the statute and/or EO that authorizes the operation of the system and the collection of PII.

(b) If direct statutory authority or an Executive Order does not exist, indirect statutory 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) If direct or indirect authority does not exist, 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 must be identified.

SORNs authorities:

10 U.S.C. 3013, Secretary of the Army; 44 U.S.C. 3101, the Federal Records Act; E.O. 12656, Assignment of Emergency Preparedness Responsibilities; DoD Directive 3020.26, Continuity of Operations Policy and Planning; Army Regulation 500-3, Army Continuity of Operations

Additional authorities:
DODI 6055.17
DoDI 5200.02
DTM 08-003
DTM 06-006
DoDM 5200.02
Final Review Recommendations of Ft. Hood Follow-on Review.
NSS Legal Opinion of Alert
Secretary of Defense MFD : Force Protection Efforts OSD010319-15/CMD013583-15

n. Does this DoD information system or electronic collection have an active and approved Office of Management and Budget (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 ☒ No ☐ Pending

(1) If "Yes," list all applicable OMB Control Numbers, collection titles, and expiration dates.
(2) If "No," explain why OMB approval is not required in accordance with DoD Manual 8910.01, Volume 2, " DoD Information Collections Manual: Procedures for DoD Public Information Collections."
(3) If "Pending," provide the date for the 60 and/or 30 day notice and the Federal Register citation.