PRIVACY IMPACT ASSESSMENT (PIA)

For the

DoD Safe Helpline
Sexual Assault Prevention and Response Office (SAPRO)

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: 14355
- ☐ **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 000100056

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 DHRA XX

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. TBD

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	TBD
Enter Expiration Date	TBD

☐ **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 U.S.C. 1561 note, Improved Sexual Assault Prevention and Response in the Armed Forces; DoD Directive 6495.01, Sexual Assault Prevention and Response (SAPR) Program; DoD Instruction 6495.02, Sexual Assault Prevention and Response (SAPR) Program Procedures.

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 DoD Safe Helpline (SHL) is to provide anonymous one-on-one support and information to victims of sexual assault under the jurisdiction of the military Services worldwide. The system also serves as a tool to track and respond to requests for SHL marketing and promotional material. The Rape, Abuse & Incest National Network (RAINN) operates the SHL under contract to the DoD. To ensure the integrity of SHL services, PII is only collected within the following SHL subcomponents:

• Material Requests (DD Form 2985-2) - Available on safehelpline.org, the voluntary Material Request Form (DD Form 2985-2) is used to request SHL marketing and promotional materials, such as brochures, coffee sleeves, and posters. The information collected includes: first and last name, shipping address, personal or work email, installation/base, rank (if applicable), status/position (e.g., Sexual Assault Response Coordinator (SARC), victim advocate, third party organization, etc.), affiliation (e.g. Service, family member, veteran, etc.), and an open comment field for questions and suggestions. Users have the option to create an account with their email and a user-selected password to place recurring orders and track the status of their current order.

• Military Feedback (DD Form 2985-1)- Available on safehelpline.org, the voluntary Military Feedback Form (DD Form 2985-1) enables individuals to leave comments, compliments, or complaints about the services of a SARC, victim advocate, or other military staff or personnel on their installation/base. Information provided on this form is forwarded to DoD SAPRO and maintained in the Victim-Related Inquiries system of record. Information collected includes: first and last name, user type (e.g. victim/survivor, family friend, etc.), Service affiliation, status/position (e.g., Service member, military spouse, DoD civilian employee, etc.), installation where the interaction took place, date of incident, the name and/or office and title of the military personnel about which the feedback is being submitted, and an open comment field which states, "If you have a complaint, or a compliment, about the service you received, please be as specific as possible." The form may also be submitted anonymously. Individuals may also simply leave their contact information (email, address, phone number) and request SAPRO contact them.

• Responder Administrative Database - A searchable referrals database that houses contact information for SARCs, medical, legal, chaplain, and military police resources, as well as information for civilian sexual assault service providers. The database maintains: name and work-related contact information (installation/ base, address, email, phone number) for each responder. Information regarding resources listed in the database may only be retrieved by authorized Safe Helpline users (i.e., appointed Service Sexual Assault Prevention and National Guard Bureau POCs) and staff by searching by name of a base, installation, state, or zip code. Information for military service providers are provided and maintained by Service SAPR and National Guard Bureau POCs. Civilian providers are vetted and their information maintained by RAINN.

• Follow-up Support Services (FSS) Database - The Follow-up Support Services Database maintains information regarding referrals discussed during an individual's call to the SHL in order to help address ongoing issues or difficulties and ensure that quality care continues when there are changes in program management/staff. Name or pseudonym, phone number, rank, base, state, and age may be required and maintained in the database in order to offer support services to individuals who have not reported their assaults to a military authority. Collecting these data fields ensures that any individual opting to receive follow-up support services from a SHL staff member can get support in a way that is most convenient for them.

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

The risks associated with the collection of PII by SHL include the threat of unauthorized access and distribution, which could lead to the degradation of information confidentiality and integrity. All individuals with access to SHL data undergo a background investigation and sign a nondisclosure agreement. Policies are in place for data backup, contingency operations, incident handling, and change management. All

information assurance (IA) personnel are required to be familiar with their prescribed roles in all IA related plans. Release of PII is controlled by the Government and will only occur in accordance with applicable law and the routine uses in the system of records of notice.

Follow-up support service records are maintained in a secure, online database. Information is stored in a redundant data center infrastructure with full featured physical security measures, including integrated closed circuit TV and a card reader/biometric security system, man trap security access for raised floor areas, exterior security cameras, and 24/7 security service. Only authorized users who are granted access can have access to software servers, which are housed in three secured cages. The servers are also equipped with an inbound / outbound network anti-virus that is monitoring against known virus and spyware.

All other records are maintained within the Amazon Web Services (AWS) network infrastructure. The protections on the network include firewalls, passwords, and web-common security architecture. AWS restricts physical access to the data centers where the SHL servers reside. Physical access logs are reviewed and analyzed on a daily basis by AWS personnel. All PII is stored in a password-protected environment with internal access only. All individuals with access to the data undergo a background investigation and sign a nondisclosure agreement.

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. Office of General Council

☒ **Other DoD Components.**

Specify. Military Police

☐ **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. Printing Vendor (Nonprofit Business Service)

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.

Voluntary, however, failure to provide information may limit SHL's ability to provide requested services.

(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.

Individuals requesting SHL services cannot give or withhold their consent to specific uses of their PII. The information collected is used only for those limited purposes which are required in order for services to be provided.

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	SHL Materials Request: Authority: 10 U.S.C. 1561 note, Improved Sexual Assault Prevention and Response in the Armed

format.

Forces; DoD Directive 6495.01, Sexual Assault Prevention and Response (SAPR) Program; DoD Instruction 6495.02, Sexual Assault Prevention and Response (SAPR) Program Procedures.

Principal Purposes(s): To track and respond to request for Safe Helpline (SHL) marketing and promotional material.

Routine Use(s): Disclosure of records are generally permitted under 5 U.S.C. 552a(b) of the Privacy Act of 1974, as amended.

To SAPRO's printing vendor to ship marketing and promotional materials requested via SHL.

Applicable Blanket Routine Use(s) are: Law Enforcement Routine Use, Congressional Inquiries Disclosure Routine Use, Disclosure to the Department of Justice for Litigation Routine Use, Disclosure of Information to the National Archives and Records Administration Routine Use, and Data Breach Remediation Purposes Routine Use.

The DoD Blanket Routine Uses set forth at the beginning of the Office of the Secretary of Defense (OSD) compilation of systems of records notices may apply to this system. The complete list of DoD Blanket Routine Uses can be found Online at: http://dpcld.defense.gov/Privacy/SORNsIndex/BlanketRoutineUses.aspx

Disclosure: Voluntary, however, failure to provide information may limit SHL's ability to provide requested services.

Military Feedback:

Authority: 10 U.S.C. 1561 note, Department of Defense Policy and Procedures on Prevention and Response to Sexual Assaults Involving Members of the Armed Forces; 10 U.S.C. 47, Uniformed Code of Military Justice; DoD Directive 6495.01, Sexual Assault Prevention and Response (SAPR) Program; DoD Instruction 6595.02, Sexual Assault Prevention and Response (SAPR) Program Procedures."

Principle Purposes: The information provided on this form will be used to facilitate and track requests for assistance received by DoD SAPRO regarding sexual assault or general information about the DoD's SAPR program. This form does not constitute a report of sexual assault.

Routine Use(s): Disclosure of records are generally permitted under 5 U.S.C. 552a(b) of the Privacy Act of 1974, as amended.

Applicable Blanket Routine Use(s) are: Law Enforcement Routine Use, Congressional Inquiries Disclosure Routine Use, Disclosure to the Department of Justice for Litigation Routine Use, Disclosure of Information to the National Archives and Records Administration Routine Use, and Data Breach Remediation Purposes Routine Use.

The DoD Blanket Routine Uses set forth at the beginning of the Office of the Secretary of Defense (OSD) compilation of systems of records notices may apply to this system. The complete list of DoD Blanket Routine Uses can be found Online at: http://dpcld.defense.gov/Privacy/SORNsIndex/BlanketRoutineUses.aspx

Disclosure: Voluntary, however, failure to provide information may limit SHL's ability to provide requested services.

For All other SHL services:

Authority: 10 U.S.C. 1561 note, Department of Defense Policy and Procedures on Prevention and Response to Sexual Assaults Involving Members of the Armed Forces; 10 U.S.C. 47, Uniformed Code of Military Justice; DoD Directive 6495.01, Sexual Assault Prevention and Response (SAPR) Program; DoD Instruction 6595.02, Sexual Assault Prevention and Response (SAPR) Program Procedures."

Principle Purposes: To provide support and information to victims of sexual assault under the jurisdiction of the military Services.

Routine Use(s): Disclosure of records are generally permitted under 5 U.S.C. 552a(b) of the Privacy Act of 1974, as amended.

Applicable Blanket Routine Use(s) are: Law Enforcement Routine Use, Congressional Inquiries Disclosure Routine Use, Disclosure to the Department of Justice for Litigation Routine Use, Disclosure of Information to the National Archives and Records Administration Routine Use, and Data Breach Remediation Purposes Routine Use.

The DoD Blanket Routine Uses set forth at the beginning of the Office of the Secretary of Defense (OSD) compilation of systems of records notices may apply to this system. The complete list of DoD Blanket Routine Uses can be found Online at: http://dpcld.defense.gov/Privacy/SORNsIndex/BlanketRoutineUses.aspx

Disclosure: Voluntary, however, failure to provide information may limit SHL's ability to provide requested services.

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.