



PRIVACY IMPACT ASSESSMENT (PIA)

For the

Defense Sexual Assault Incident Database (DSAID)

Office of the Under Secretary of Defense for Personnel and Readiness (OUSDP&R),
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
- 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

0704-0482

Enter Expiration Date

06/30/2012

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 (U.S.C.) 113 note, Department of Defense Policy and Procedures on Prevention and Response to Sexual Assaults Involving Members of the Armed Forces; 10 U.S.C. 136, Under Secretary of Defense for Personnel and Readiness; 32 U.S.C., National Guard; DoD Directive 6495.01, Sexual Assault Prevention and Response (SAPR) Program; DoD Instruction 6495.02, Sexual Assault Prevention and Response (SAPR) Program Procedures; 10 U.S.C. 3013, Secretary of the Army; Army Regulation 600-20, Sexual Assault Prevention and Response (SAPR) Program; 10 U.S.C. 5013, Secretary of the Navy; Secretary of the Navy Instruction 1752.4A, Sexual Assault Prevention and Response; Marine Corps Order 1752.5A, Sexual Assault Prevention and Response (SAPR) Program; 10 U.S.C. 8013, Secretary of the Air Force; Air Force Instruction 36-6001, Sexual Assault Prevention and Response (SAPR) Program; and E.O. 9397 (SSN), as amended.

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.

To facilitate the reporting requirements found in 10 U.S.C. 113, note, DSAID will centralize case-level sexual assault data involving a member of the Armed Forces, in a manner consistent with Department of Defense (DoD) regulations for Unrestricted and Restricted Reporting, and maintenance of information regarding sexual assaults involving a member of the Armed Forces, including information, if available, about the nature of the assault, the victim, the alleged perpetrator, and case outcomes in connection with the assault.

The system will include the capability for entering records and interfacing data; generating various level reports and queries; and conducting case and business management.

In records and data in cases involving a Unrestricted Report, victim information will include: last name, first name, middle name, victim case number (i.e. system generated unique control number), identification type (i.e. social security number (SSN), passport, U.S. Permanent Residence Card, foreign identification), identification number for type of identification type referenced, birth date, age at the time of incident, gender, race, ethnicity, and victim type (i.e. military, DoD civilian/contractor).

In records and data in cases involving a Unrestricted Report, alleged perpetrator information will include: last name, first name, middle name, identification type (i.e. SSN, passport, U.S. Permanent Residence Card, foreign identification), identification number for type of identification type referenced, birth date, age at the time of incident, gender, race, ethnicity, and subject type (i.e. military, DoD civilian/contractor).

In records and data in cases involving a Restricted Report, no personally identifying information will be included in victim or alleged perpetrator information.

At the Military Service level, Sexual Assault Response Coordinators (SARC) and Sexual Assault Prevention and Response Victim Advocates (SAPR VA) will work with victims to ensure that they are aware of services available and have contact with medical treatment personnel and DoD law enforcement entities. At the DoD level, only de-identified information will be used to respond to mandated reporting requirements.

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

DSAID will collect data, in a manner consistent with DoD regulations for Unrestricted and Restricted Reporting, and maintain information regarding sexual assaults involving a member of the Armed Forces, including information, if available, about the nature of the assault, the victim, the alleged perpetrator, and case outcomes in connection with the assault. As a result, PII contained in DSAID could identify individuals as either victims or alleged perpetrator of a sexual assault involving a member of the Armed Forces.

In order to safeguard individual privacy, records will be maintained in a controlled facility. Physical entry will be restricted by the use of alarms, cipher and 509 locks, armed guards, and slow access. Access to case files in the system will be role-based and require the use of a Common Access Card and associated personal identification number (PIN). Further, at the DoD-level, only de-identified data for open cases will be able to be accessed.

DSAID will reside on the Office of the Secretary of Defense network. The protections on the network will include firewalls, passwords, and web-common security architecture. In addition, the local drive will reside behind the firewall on the safe side; the direct database will not be able to be accessed from the outside; and the system will rest on the Nonsecure Internet Protocol Router Network.

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.

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.

Victims will be asked for their information by SARCs. Victims of sexual assault have two options when reporting information regarding an incident. Individuals may consent to a full collection of information, which will initiate legal proceedings, by making an Unrestricted Report. Or they may make a Restricted Report that enables them to receive assistance without legal obligation. If a victim of a sexual assault involving a member of the Armed Forces makes a Restricted Report of sexual assault, no personally identifying information for the victim is collected.

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

In an Unrestricted Report, alleged perpetrators of sexual assault do not have the opportunity to object to the collection of their personally identifying information, as they do not provide this information directly to users of DSAID. Case information maintained in DSAID is received, when appropriate, from Military Service-specific systems that capture sexual assault data to include Military Criminal Investigative Organizations' and Military Service sexual assault case management systems.

In a Restricted Report, no personally identifying information for the alleged perpetrator is collected.

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.

Victims will be asked for their information by SARCs. Victims of sexual assault have two options when reporting information regarding an incident. Individuals may consent to a full collection of information, which will initiate legal proceedings, by making an Unrestricted Report. Or they may make a Restricted Report that enables them to receive assistance without legal obligation. If a victim of a sexual assault involving a member of the Armed Forces makes a Restricted Report of sexual assault, no personally identifying information for the victim is collected.

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

In an Unrestricted Report, alleged perpetrators of sexual assault do not have the opportunity to consent to the specific uses of their personally identifying information, as they do not provide this information directly to users of DSAID. Case information maintained in DSAID is received, when appropriate, from Military Service-specific systems that capture sexual assault data to include Military Criminal Investigative Organizations' and Military Service sexual assault case management systems.

In a Restricted Report, no personally identifying information for the alleged perpetrator is collected.

k. What information is provided to an individual when asked to provide PII data? Indicate all that apply.

- | | |
|---|---|
| <input checked="" type="checkbox"/> Privacy Act Statement | <input type="checkbox"/> Privacy Advisory |
| <input type="checkbox"/> Other | <input type="checkbox"/> None |

Describe each applicable format.

SARCs will read victims the Privacy Act Statement when they elect to report on the DD Form 2910, "Victim Reporting Preference Statement."

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.

The system will hold the following principal information: victim of a sexual assault involving a member of the Armed Forces; alleged perpetrator in a sexual assault involving a member of the Armed Forces; incident information; and case outcomes in connection with the assault.

In records and data in cases involving a Unrestricted Report, victim information will include: last name, first name, middle name, victim case number (i.e. system generated unique control number), identification type (i.e. social security number (SSN), passport, U.S. Permanent Residence Card, foreign identification), identification number for type of identification type referenced, birth date, age at the time of incident, gender, race, ethnicity, and victim type (i.e. military, DoD civilian/contractor).

In records and data in cases involving a Unrestricted Report, alleged perpetrator information will include: last name, first name, middle name, identification type (i.e. SSN, passport, U.S. Permanent Residence Card, foreign identification), identification number for type of identification type referenced, birth date, age at the time of incident, gender, race, ethnicity, and subject type (i.e. military, DoD civilian/contractor).

In records and data in cases involving a Restricted Report, no personally identifying information will be included in victim or alleged perpetrator information.

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

Victims will be asked for their information by SARCs.

Case information maintained in DSAID is received, when appropriate, from Military Service-specific systems that capture sexual assault data to include Military Criminal Investigative Organizations' and Military Service sexual assault case management systems to include the following:

The Department of the Army. Sexual Assault Data Management System.
The Department of the Navy. Consolidated Law Enforcement Operations Center.
The Department of the Air Force. Investigative Information Management System.

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

- | | |
|--|--|
| <input checked="" type="checkbox"/> Paper Form | <input checked="" type="checkbox"/> Face-to-Face Contact |
| <input checked="" type="checkbox"/> Telephone Interview | <input type="checkbox"/> Fax |
| <input type="checkbox"/> Email | <input type="checkbox"/> Web Site |
| <input checked="" type="checkbox"/> Information Sharing - System to System | |
| <input type="checkbox"/> Other | |

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

Identification and data matching.

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

Mission-related use.

The system will include the capability for entering records and interfacing data; generating various level reports and queries; and conducting case and business management.

When implemented, DSAID will enhance the transparency of sexual assault-related data, while providing privacy for restricted reporting options for sexual assault victims; provide accurate and timely reporting of sexual assault incidents; use data as an enabler to enhance analysis and trend identification capabilities; and allow for evaluation of DoD SAPRO and Service Sexual Assault Prevention and Response program effectiveness.

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.

Data will not be broken out into personal descriptors. It will remain in numerical form.

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

During the testing phase, developers will utilize information to ensure that the system performs the appropriate functionalities. Additionally, contractors serving in a system administration role may access PII to resolve issues within the system. In no circumstance will individuals access PII for other than a need-to-know basis.

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

Records will be maintained in a controlled facility. Physical entry is restricted by the use of alarms, cipher and 509 locks, armed guards, and slow access. Access to case files in the system will be role-based and require the use of a Common Access Card and associated PIN. Further, at the DoD-level, only de-identified data for open cases can be accessed.

(2) Technical Controls. Indicate all that apply.

User Identification Biometrics
 Password Firewall

- Intrusion Detection System (IDS)
- Encryption
- External Certificate Authority (CA) Certificate
- Other
- Virtual Private Network (VPN)
- DoD Public Key Infrastructure Certificates
- Common Access Card (CAC)

System access to case files will be limited to the victim's SARC and Sexual Assault Prevention and Response program managers. DSAID will sit on the Office of the Secretary of Defense network. The protections on the network will include firewalls, passwords, and web-common security architecture. In addition, the local drive will reside behind the firewall on the safe side, the direct database will not be able to be accessed from the outside, and the system will rest on the Nonsecure Internet Protocol Router Network.

(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

Access roles and permission lists for SARCs will be granted by Service Sexual Assault Prevention and Response program managers through the assignment of appropriate user roles. At the DoD-level, only de-identified data for open cases will be able to be accessed.

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:

| | | | |
|-------------------------------------|---|---------------|------------|
| <input checked="" type="checkbox"/> | Authorization to Operate (ATO) | Date Granted: | 03/21/2012 |
| <input type="checkbox"/> | Interim Authorization to Operate (IATO) | Date Granted: | |
| <input type="checkbox"/> | Denial of Authorization to Operate (DATO) | Date Granted: | |
| <input type="checkbox"/> | 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?

Collection: PII information will be collected by SARCs. The collection of records will be used to document elements of the sexual assault response and reporting process and comply with the procedures in place to effectively manage the Sexual Assault Prevention and Response program.

Use, Retention, and Processing: These will be For Official Use Only records and will be maintained in controlled facilities that employ physical restrictions and safeguards such as security guards, identification badges, key cards, and locks. Records will be kept in DSAID for retrieval and analysis purposes for 50 years, after which records will be destroyed in a way that precludes recognition or reconstruction in accordance with DoD 5200.1-R, "Information Security Program."

Disclosure: No other personnel other than those with role-based access will have access to member's PII unless permission is granted from the individual in writing to release the information.

Destruction: For Official Use Only records will be destroyed in a way that precludes recognition or reconstruction that includes but are not limited to the following methods: burning, cross-cut shredding, wet-pulping, mutilation, chemical decomposition or according to DoD 5200.1-R, "Information Security Program."

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

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

Access Controls: Role-based access and Common Access Card enabled functionality will limit access to the application and/or specific functional areas of the application.

Confidentiality: PII data in transit to or held in DSAID will not be made available or disclosed to unauthorized individuals, entities, or processes through encryption and firewall protection. Non-aggregated data will not be able to be stored on local hard drives or thumb drives and will be immobile.

Integrity: Data in DSAID will be protected through the above access controls to ensure that it has not been altered or destroyed in an unauthorized manner.

Audits: Audits will review and examine records, activities, and system parameters to assess the adequacy of maintaining, managing, and controlling events that may degrade the security posture of DSAID's following capabilities: reporting, data entry/case management, interfacing, and business management.

Training: Security training will be provided to educate users to DSAID's security requirements. The system will display reminders to ensure users remain aware of their responsibilities to protect PII.

Physical Security: In order to safeguard individual privacy, records will be maintained in a controlled facility.

SECTION 4: REVIEW AND APPROVAL SIGNATURES

Prior to the submission of the PIA for review and approval, the PIA must be coordinated by the Program Manager or designee through the Information Assurance Manager and Privacy Representative at the local level.

Program Manager or Designee Signature

SULLIVAN.DARLENE.L.1132765134
Digitally signed by SULLIVAN.DARLENE.L.1132765134
DN: c=US, o=U.S. Government, ou=DoD, ou=PKI, ou=DODHRA,
cn=SULLIVAN.DARLENE.L.1132765134
Date: 2012.03.06 09:03:31 -05'00'

Name:

Ms. Darlene Sullivan

Title:

Oversight Program Manager

Organization:

Sexual Assault Prevention and Response Office

Work Telephone Number:

(703) 696-8695

DSN:

Email Address:

darlene.sullivan@wso.whs.mil

Date of Review:

03/06/2012

Other Official Signature (to be used at Component discretion)

Digitally signed by RUSHIN JR.EDWARD.E.1030992187
DN: c=US, o=U.S. Government, ou=DoD, ou=PKI, ou=DODHRA,
cn=RUSHIN JR.EDWARD.E.1030992187

Name:

Mr. Edward Rushin

Title:

Deputy Director for Operations

Organization:

Sexual Assault Prevention and Response Office

Work Telephone Number:

(703) 696-9429

DSN:

Email Address:

edward.rushin@wso.whs.mil

Date of Review:

03/06/2012

**Other Official Signature
(to be used at Component
discretion)**

Name:

Title:

Organization:

Work Telephone Number:

DSN:

Email Address:

Date of Review:

**Component Senior
Information Assurance
Officer Signature or
Designee**

**KENNEDY.GEOR
GE.L.1200888908**

Digitally signed by
KENNEDY.GEORGE.L.1200888908
DN: c=US, o=U.S. Government, ou=DoD,
ou=PKI, ou=WHS,
cn=KENNEDY.GEORGE.L.1200888908
Date: 2012.05.10 07:57:24 -04'00'

Name:

Title:

Organization:

Work Telephone Number: 5713720201

DSN:

Email Address:

Date of Review:

George Lee Kennedy

Senior Information Assurance Officer

EITSD

lee.kennedy@osd.mil

10 May 2012

**Component Privacy Officer
Signature**

**ALLARD.CINDY.
L.1231656614**

Digitally signed by ALLARD.CINDY.L.1231656614
DN: c=US, o=U.S. Government, ou=DoD, ou=PKI,
ou=WHS, cn=ALLARD.CINDY.L.1231656614
Date: 2012.05.04 14:51:46 -04'00'

Name:

Title:

Organization:

Work Telephone Number: 571-372-0461

DSN:

Email Address:

Date of Review:

Cindy L. Allard

Chief, OSD/JS Privacy Office

WHS/ESD/FOID

cindy.allard@whs.mil

4 May 2012

Component CIO Signature
(Reviewing Official)

Ronald Bechtold

Name:

RONALD BECHTOLD

Title:

OSD CIO

Organization:

EITSD

Work Telephone Number:

703-692-7455

DSN:

Email Address:

RONALD.BECHTOLD@OSD.MIL

Date of Review:

5/16/12

Publishing:

Only Sections 1 and 2 of this PIA will be published. Each DoD Component will maintain a central repository of PIAs on the Component's public Web site. DoD Components will submit an electronic copy of each approved PIA to the DoD CIO at: pia@osd.mil.

If the PIA document contains information that would reveal sensitive information or raise security concerns, the DoD Component may restrict the publication of the assessment to include Sections 1 and 2.