

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:

Defense Sexual Assault Incident Database (DSAID)

2. DOD COMPONENT NAME:

Under Secretary of Defense for Personnel and Readiness

3. PIA APPROVAL DATE:

07/03/18

Sexual Assault Prevention and Response Office (SAPRO)

SECTION 1: PII DESCRIPTION SUMMARY (FOR PUBLIC RELEASE)

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

- | | |
|------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------|
| <input type="checkbox"/> From members of the general public | <input type="checkbox"/> From Federal employees and/or Federal contractors |
| <input checked="" type="checkbox"/> From both members of the general public and Federal employees and/or Federal contractors | <input type="checkbox"/> Not Collected (if checked proceed to Section 4) |

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

- | | |
|-----------------------------------------------------------------------------------|---------------------------------------------------------|
| <input type="checkbox"/> New DoD Information System | <input type="checkbox"/> New Electronic Collection |
| <input type="checkbox"/> Existing DoD Information System | <input type="checkbox"/> Existing Electronic Collection |
| <input checked="" type="checkbox"/> 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.

To centralize case-level sexual assault data involving a member of the Armed Forces, in a manner consistent with statute and DoD regulations for Unrestricted and Restricted reporting. To facilitate reports to Congress on claims of retaliation in connection with a Unrestricted Report of sexual assault made by or against a member of the Armed Force.

Records may also be used as a management tool for statistical analysis, tracking, reporting, evaluating program effectiveness, conducting research, and case and business management. De-identified data may also be used to respond to mandated reporting requirements.

Victim and alleged perpetrator information includes: Age at the time of incident; gender, race, ethnicity; affiliation (e.g., military, DoD civilian/contractor, other government employee, U.S. civilian, foreign national/military, unknown, and military dependent); Service, grade/rank, status (e.g., Active Duty, Reserve, National Guard); and location of assignment and incident. Additional victim and alleged perpetrator information, maintained in Unrestricted Reports only, includes: full name; identification type and number (e.g., DoD Identification number, Social Security Number, passport, U.S. Permanent Residence Card, foreign identification); and date of birth.

Additional victim information includes: Defense Sexual Assault Incident Database (DSAID) control number (i.e., system generated unique control number); and relationship to alleged perpetrator. Additional victim information maintained in Unrestricted Reports only includes: Work or personal contact information (e.g., phone number, address, email address); and name of commander.

For Restricted Reports (reports that do not initiate investigation), no personally identifying information for the victim and/or alleged perpetrator, and no information on reports of retaliation is maintained in DSAID.

Other sexual assault data collected to support case and business management includes: Date and type of report (e.g., Unrestricted or Restricted); tracking information on Sexual Assault Forensic Examinations performed, and referrals to appropriate resources; information on line of duty determinations; victim safety information; case management meeting information; and information on memoranda of understanding. For Unrestricted reports, information on expedited transfers and civilian/military protective orders may also be collected.

Retaliation reporter and alleged retaliator information includes: full name; identification type and number (e.g., DoD Identification number, Social Security Number, passport, U.S. Permanent Residence Card, foreign identification); date of birth; gender, race, ethnicity; affiliation (e.g., military, DoD civilian/contractor, other government employee, and military dependent); duty status, pay grade; location of assignment. Additional retaliation reporter information includes: retaliation control number (i.e., system generated unique control number).

Other retaliation data collected to support case and business management includes: DSAID control number, tracking information on actions take to support reporter of retaliation; nature and findings of the retaliation investigation; and relationship between alleged retaliator and

retaliation reporter and alleged retaliation and alleged perpetrator of sexual assault.

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)

Identification and verification

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.

Sexual assault victims are asked for their information by Sexual Assault Response Coordinators (SARCs) and must sign a DD2910, "Victim Reporting Preference Statement" to initiate an official report. When reporting information regarding a sexual assault incident victims have two options, Restricted or Unrestricted reporting. 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 or maintained.

Reports of retaliation may only be made in connection with an Unrestricted Report of sexual assault made by or against a member of the Armed Force. Retaliation reporters must sign DDXXXX, "[Insert Name Here]" to initiate an official report.

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.

Sexual assault victims are asked for their information by SARCs and must elect one of two reporting options, Restricted or Unrestricted.

Restricted reporting allows sexual assault victims to confidentially disclose the assault to specified individuals (i.e., SARC, SAPR Victim Advocate (VA), or healthcare personnel) and receive medical treatment, including emergency care, counseling, and assignment of a SARC and SAPR VA, without triggering an official investigation. The victim's report provided to healthcare personnel (including the information acquired from a Sexual Assault Forensic Examination Kit), SARCs, or SAPR VAs are not reported to law enforcement or to the command to initiate an official investigation unless the victim consents or an established exception applies in accordance with DoD Instruction 6495.02, "Sexual Assault Prevention and Response (SAPR) Program Procedures."

Unrestricted reporting allows a victim to disclose, without requesting confidentiality or Restricted Reporting, that he or she is the victim of a sexual assault. Under these circumstances, the victim's report provided to healthcare personnel, the SARC, a SAPR VA, command authorities, or other persons is reported to law enforcement and may be used to initiate an official investigative process.

Reports of retaliation may only be made in connection with an Unrestricted Report of sexual assault made by or against a member of the Armed Force. Retaliation reporters, however, do not have the option to confidentially disclose the retaliation. All official reports of retaliation will be maintained in DSAID and include the reporters PII.

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

SARCs read victims the Privacy Act Statement when they elect to report on the DD Form 2910, "Victim Reporting Preference Statement," which states the following:

AUTHORITY: 10 U.S.C. 136, Under Secretary of Defense for Personnel and Readiness; 10 U.S.C. 3013, Secretary of the Army; 10 U.S.C. 5013, Secretary of the Navy; 10 U.S.C. 8013, Secretary of the Air Force; 32 U.S.C. 102, 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; Army Regulation 600-20, Chapter 8, Army Command Policy (Sexual Assault Prevention and Response Program); Secretary of the Navy Instruction 1752.4B, Sexual Assault Prevention and Response; Marine Corps Order 1752.5B, Sexual Assault Prevention and Response (SAPR) Program; Air Force Instruction 90-6001, Sexual Assault Prevention and Response (SAPR) Program; and E.O. 9397 (SSN), as amended.

PRINCIPAL PURPOSE(S): Information will be used to document elements of the sexual assault response and/or reporting process and comply with the procedures set up to effectively manage the sexual assault prevention and response program. At the local level, Service SAPR Program Management, Major Command Sexual Assault Response Coordinator(s) (SARCs), Installation and Brigade SARCs use information to ensure that victims are aware of services available and have contact with medical treatment personnel and DoD law enforcement entities. At the DoD level, only de-identified data is used to respond to mandated congressional reporting requirements. The

DoD Sexual Assault Prevention and Response Office has access to identified closed case information and de-identified, aggregate open case information for congressional reporting, study, research, and analysis purposes.

ROUTINE USE(S): Disclosure of records are generally permitted under 5 U.S.C. 552a(b) of the Privacy Act of 1974, as amended. Routine uses may be found in the applicable system of records notice, DHRA 06, Defense Sexual Assault Incident Database, at <http://dpcl.d.defense.gov/Privacy/SORNsIndex/DOD-wide-SORN-Article-View/Article/570559/dhra-06-dod/>

DISCLOSURE: Voluntary. However, if you decide not to provide certain information, it may impede the ability of the SARC to offer the full range of care and support established by the Sexual Assault Prevention and Response program. You will not be denied advocacy services or healthcare (medical and mental health) because you selected the Restricted Reporting option. The Social Security Number (SSN) is one of several unique personal identifiers that may be provided. This form will be retained for 50 years.

DD2965, "Defense Sexual Assault Incident Database (DSAID) Data Form" also states:

AUTHORITY: 10 U.S.C. 136, Under Secretary of Defense for Personnel and Readiness; 10 U.S.C. 3013, Secretary of the Army; 10 U.S.C. 5013, Secretary of the Navy; 10 U.S.C. 8013, Secretary of the Air Force; 32 U.S.C. 102, 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; Army Regulation 600-20, Chapter 8, Army Command Policy (Sexual Assault Prevention and Response Program); Secretary of the Navy Instruction 1752.4B, Sexual Assault Prevention and Response; Marine Corps Order 1752.5B, Sexual Assault Prevention and Response (SAPR) Program; Air Force Instruction 90-6001, Sexual Assault Prevention and Response (SAPR) Program; and E.O. 9397 (SSN), as amended.

PRINCIPAL PURPOSE(S): The information collected documents elements of the sexual assault response and/or reporting process and will be entered into the Defense Sexual Assault Incident Database to comply with the procedures set up to effectively manage the sexual assault prevention and response program. At the local level, Service SAPR Program Management, Major Command Sexual Assault Response Coordinator(s) (SARCs) and Installation SARC(s) use this information to ensure that victims are aware of services available and have contact with medical treatment personnel and DoD law enforcement entities. At the DoD level, only de-identified data is used to respond to mandated congressional reporting requirements. The DoD Sexual Assault Prevention and Response Office has access to identified closed case information and de-identified, aggregate open case information for congressional reporting, study, research, and analysis purposes.

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 permit the disclosure of records of closed cases of unrestricted reports to the Department of Veterans Affairs (DVA) for purpose of providing medical care to former Service members and retirees, to determine the eligibility for or entitlement to benefits, and to facilitate collaborative research activities between the DoD and DVA.

Routine uses may be found in the applicable system of records notice, DHRA 06, Defense Sexual Assault Incident Database, at <http://dpcl.d.defense.gov/Privacy/SORNsIndex/DOD-wide-SORN-Article-View/Article/570559/dhra-06-dod/>

DISCLOSURE: Voluntary. However, if you decide not to provide certain information, it may impede the ability of the SARC to offer the full range of care and support established by the sexual assault prevention and response program. You will not be denied benefits via the Restricted Reporting option. For Unrestricted Reports, the Social Security Number (SSN) is one of several unique personal identifiers that may be provided. Some alternatives include state driver's license number, passport number, or DoD ID number.

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.

Other DoD Components

Specify.

SAPR Program Managers, Sexual Assault Response Coordinators, and authorized Legal Officers (i.e. attorneys provided access to the system) of the Army, Navy, Marine Corps, Air Force, and National Guard Bureau; DoD, Army, Navy, Air Force, and Office of the Inspector General

Other Federal Agencies

Specify.

Department of Veterans Affairs

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)
- | | |
|----------------------------------------------------------------------|---------------------------------------------|
| <input checked="" type="checkbox"/> Individuals | <input type="checkbox"/> Databases |
| <input checked="" type="checkbox"/> Existing DoD Information Systems | <input type="checkbox"/> Commercial Systems |
| <input type="checkbox"/> Other Federal Information Systems | |

Army Law Enforcement Reporting and Tracking System (Army), Consolidated Law Enforcement Operations Center (Navy), and Investigative Information Management System (Air Force)

- j. How will the information be collected?** (Check all that apply and list all Official Form Numbers if applicable)
- | | |
|-----------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------|
| <input type="checkbox"/> E-mail | <input checked="" type="checkbox"/> Official Form (Enter Form Number(s) in the box below) |
| <input checked="" type="checkbox"/> Face-to-Face Contact | <input type="checkbox"/> Paper |
| <input type="checkbox"/> Fax | <input checked="" type="checkbox"/> Telephone Interview |
| <input checked="" type="checkbox"/> Information Sharing - System to System | <input type="checkbox"/> Website/E-Form |
| <input type="checkbox"/> Other (If Other, enter the information in the box below) | |

DD Form 2910; DD Form 2965; DD 2910-1

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

SORN Identifier, not the Federal Register (FR) Citation. Consult the DoD Component Privacy Office for additional information or <http://dpcl.dod.mil> 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.

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

(3) Retention Instructions.

Temporary, Cutoff cases at the end of the fiscal year. Destroy 50 years after cutoff.

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 statute 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.

10 U.S.C. 136, Under Secretary of Defense for Personnel and Readiness; 10 U.S.C. 3013, Secretary of the Army; 10 U.S.C. 5013, Secretary of the Navy; 10 U.S.C. 8013, Secretary of the Air Force; 32 U.S.C. 102, 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; Army Regulation 600-20, Chapter 8, Army Command Policy (Sexual Assault Prevention and Response Program); Secretary of the Navy Instruction 1752.4B, Sexual Assault Prevention and Response; Marine Corps Order 1752.5B, Sexual Assault Prevention and Response (SAPR) Program; Air Force Instruction 90-6001, Sexual Assault Prevention and Response (SAPR) Program; and E.O. 9397 (SSN), as amended.

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.

0704-0482, Defense Sexual Assault Incident Database, Expiration Date: 11/30/2018

SECTION 2: PII RISK REVIEW

a. What PII will be collected (a data element alone or in combination that can uniquely identify an individual)? (Check all that apply)

- | | | |
|------------------------------------------------------------|--------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------|
| <input type="checkbox"/> Biometrics | <input checked="" type="checkbox"/> Birth Date | <input type="checkbox"/> Child Information |
| <input type="checkbox"/> Citizenship | <input type="checkbox"/> Disability Information | <input checked="" type="checkbox"/> DoD ID Number |
| <input type="checkbox"/> Driver's License | <input type="checkbox"/> Education Information | <input type="checkbox"/> Emergency Contact |
| <input checked="" type="checkbox"/> Employment Information | <input type="checkbox"/> Financial Information | <input checked="" type="checkbox"/> Gender/Gender Identification |
| <input checked="" type="checkbox"/> Home/Cell Phone | <input checked="" type="checkbox"/> Law Enforcement Information | <input type="checkbox"/> Legal Status |
| <input checked="" type="checkbox"/> Mailing/Home Address | <input type="checkbox"/> Marital Status | <input checked="" type="checkbox"/> Medical Information |
| <input checked="" type="checkbox"/> Military Records | <input type="checkbox"/> Mother's Middle/Maiden Name | <input checked="" type="checkbox"/> Name(s) |
| <input type="checkbox"/> Official Duty Address | <input type="checkbox"/> Official Duty Telephone Phone | <input checked="" type="checkbox"/> Other ID Number |
| <input checked="" type="checkbox"/> Passport Information | <input checked="" type="checkbox"/> Personal E-mail Address | <input type="checkbox"/> Photo |
| <input type="checkbox"/> Place of Birth | <input checked="" type="checkbox"/> Position/Title | <input type="checkbox"/> Protected Health Information (PHI) ¹ |
| <input checked="" type="checkbox"/> Race/Ethnicity | <input checked="" type="checkbox"/> Rank/Grade | <input type="checkbox"/> Religious Preference |
| <input type="checkbox"/> Records | <input type="checkbox"/> Security Information | <input checked="" type="checkbox"/> Social Security Number (SSN) (Full or in any form) |
| <input checked="" type="checkbox"/> Work E-mail Address | <input checked="" type="checkbox"/> If Other, enter the information in the box below | |

Victim and alleged perpetrator information includes: Age at the time of incident; affiliation (e.g., military, DoD civilian/contractor, other government employee, U.S. civilian, foreign national/military, unknown, and military dependent); and location of assignment and incident.

Additional victim information includes: Defense Sexual Assault Incident Database (DSAID) control number (i.e., system generated unique control number); and relationship to alleged perpetrator.

Other sexual assault data collected to support case and business management includes: Date and type of report (e.g., Unrestricted or Restricted); tracking information on Sexual Assault Forensic Examinations performed, and referrals to appropriate resources; information on line of duty determinations; victim safety information; case management meeting information; and information on memoranda of understanding. For Unrestricted reports, information on expedited transfers and civilian/military protective orders may also be collected.

Retaliation reporter and alleged retaliator information includes: affiliation (e.g., military, DoD civilian/contractor, other government employee, and military dependent); duty status; location of assignment. Additional retaliation reporter information includes: retaliation control number (i.e., system generated unique control number).

Other retaliation data collected to support case and business management includes: DSAID control number, tracking information on actions take to support reporter of retaliation; nature and findings of the retaliation investigation; and relationship between alleged retaliator and retaliation reporter and alleged retaliation and alleged perpetrator of sexual assault.

If the SSN is collected, complete the following questions.

(DoD Instruction 1000.30 states that all DoD personnel shall reduce or eliminate the use of SSNs wherever possible. SSNs shall not be used in spreadsheets, hard copy lists, electronic reports, or collected in surveys unless they meet one or more of the acceptable use criteria.)

(1) Is there a current (dated within two (2) years) DPCLTD approved SSN Justification on Memo in place?

- Yes No

If "Yes," provide the signatory and date approval. If "No," explain why there is no SSN Justification Memo.

Revised memo submitted to DPCLTD on June 27, 2018.

(2) Describe the approved acceptable use in accordance with DoD Instruction 1000.30 "Reduction of Social Security Number (SSN) Use within DoD".

The use case justifying the collection of the SSN in DSAID and on the DD Form 2965 is "Legacy System Interface" as outlined in DoD Instruction 1000.30, Enclosure 2, paragraph 2c(11). DSAID must continue to interface with Military Criminal Investigative Organization (MCIO) case management systems, which are legacy systems. Specifically, DSAID must interface weekly with the Department of the Army Law Enforcement Reporting and Tracking System, the Department of the Navy Consolidated Law Enforcement Operations Center, and the Department of the Air Force Investigative Information Management System to capture case investigation data required for congressional reporting. These legacy systems report and track individuals, and make application information available to other agencies through the use of the SSN. The use of the SSN allows data matching and verification to be conducted to ensure the correct sexual assault case information is being pushed from the MCIO system to DSAID.

(3) Describe the mitigation efforts to reduce the use including visibility and printing of SSN in accordance with DoD Instructoin 1000.30, "Reduction of Social Security Number (SSN) Use within DoD".

SAPRO takes safeguarding SSNs and other personally identifiable information collected and maintained in the system seriously. DSAID records are maintained in a controlled facility. Physical entry is restricted by the use of guards, identification badges, key cards, and locks. Access to case files in the system is role-based and requires the use of a Common Access Card, password, and can only be accessed from a .mil account.

DSAID continues to reside on the Office of the Secretary of Defense network. The protections on the network include firewalls, passwords, encryption of data, and use of a virtual private network. The local drive resides behind the firewall on the safe side and the direct database cannot be accessed from the outside. The system rests on the Nonsecure Internet Protocol Router Network. DSAID completed and met the requirements of the DoD Information Assurance Certification and Accreditation Process, receiving accreditation and authority to operate on 4 April 2016.

(4) Has a plan to eliminate the use of the SSN or mitigate its use and or visibility been identified in the approved SSN Justification request?

If "Yes," provide the unique identifier and when can it be eliminated?

If "No," explain.

Yes No

The legacy MCIO systems with which DSAID interfaces continue to use the SSN as the primary form of identification collected. The inclusion of the SSN in DSAID, therefore, remains necessary for the successful interface between DSAID and these systems. Once the legacy MCIO systems transition from the use of the SSN to another primary form of identification (e.g. the DoD Identification Number), DSAID will also transition from the use of the SSN. SAPRO, in coordination with the DSAID Change Control Board, will continue to assess options for removal of the SSN as they become available.

b. What is the PII confidentiality impact level²? Low Moderate High

¹The definition of PHI involves evaluating conditions listed in the HIPAA. Consult with General Counsel to make this determination.

²Guidance on determining the PII confidentiality impact level, see Section 2.5 "Categorization of PII Using NIST SP 800-122." Use the identified PII confidentiality impact level to apply the appropriate Privacy Overlay low, moderate, or high. This activity may be conducted as part of the categorization exercise that occurs under the Risk Management Framework (RMF). Note that categorization under the RMF is typically conducted using the information types described in NIST Special Publication (SP) 800-60, which are not as granular as the PII data elements listed in the PIA table. Determining the PII confidentiality impact level is most effective when done in collaboration with the Information Owner, Information System Owner, Information System Security Manager, and representatives from the security and privacy organizations, such as the Information System Security Officer (ISSO) and Senior Component Official for Privacy (SCOP) or designees.

c. How will the PII be secured?

(1) Physical Controls. (Check all that apply)

- | | |
|-------------------------------------------------------|---------------------------------------------------------------------------|
| <input checked="" type="checkbox"/> Cipher Locks | <input type="checkbox"/> Closed Circuit TV (CCTV) |
| <input checked="" type="checkbox"/> Combination Locks | <input checked="" type="checkbox"/> Identification Badges |
| <input checked="" type="checkbox"/> Key Cards | <input type="checkbox"/> Safes |
| <input checked="" type="checkbox"/> Security Guards | <input type="checkbox"/> If Other, enter the information in the box below |

(2) Administrative Controls. (Check all that apply)

- Backups Secured Off-site
- Encryption of Backups
- Methods to Ensure Only Authorized Personnel Access to PII
- Periodic Security Audits
- Regular Monitoring of Users' Security Practices
- If Other, enter the information in the box below

(3) Technical Controls. (Check all that apply)

- | | | |
|----------------------------------------------------------------|-----------------------------------------------------------|--------------------------------------------------------------------------------|
| <input type="checkbox"/> Biometrics | <input type="checkbox"/> Common Access Card (CAC) | <input checked="" type="checkbox"/> DoD Public Key Infrastructure Certificates |
| <input checked="" type="checkbox"/> Encryption of Data at Rest | <input type="checkbox"/> Encryption of Data in Transit | <input type="checkbox"/> External Certificate Authority Certificates |
| <input checked="" type="checkbox"/> Firewall | <input type="checkbox"/> Intrusion Detection System (IDS) | <input type="checkbox"/> Least Privilege Access |

- Role-Based Access Controls Used Only for Privileged (Elevated Roles) User Identification and Password
 Virtual Private Network (VPN) If Other, enter the information in the box below

d. What additional measures/safeguards have been put in place to address privacy risks for this information system or electronic collection?

Access rights and permission lists for Sexual Assault Response Coordinators (SARCs) and authorized Military Service legal officers are granted by Military Service Sexual Assault Prevention and Response program managers through the assignment of appropriate user roles. Access is further restricted to authorized users on the Nonsecure Internet Protocol Router Network and with a CAC. In addition, the local drive resides behind a firewall and the direct database cannot be accessed from the outside.