

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 Advocate Certification Program

2. DOD COMPONENT NAME:

Defense Human Resources Activity

3. PIA APPROVAL DATE:

09/04/20

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 checked="" type="checkbox"/> From Federal employees and/or Federal contractors |
| <input 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 checked="" type="checkbox"/> Existing DoD Information System | <input type="checkbox"/> Existing Electronic Collection |
| <input 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 track the certification of Sexual Assault Response Coordinator (SARC) and Sexual Assault Prevention and Response Victim Advocate (SAPR VAs). System information will be used to review, process, and report on the status of SARC and SAPR VA certifications to Congress.

Information collected includes: Applicant's first name, middle initial, and last name; position type (DoD personnel); Service/DoD affiliation and status; grade/rank; installation/command; work email address and telephone number; official military address of applicant and applicant's SARC (commanding officer, street, city, state, ZIP code, country); position level (Level I, II, III, or IV); certificates of training; date of application; verification of sexual assault victim advocacy experience (position, dates, hours, supervisor; name, title, and work telephone number of verifier); evaluation of sexual assault victim advocacy experience (description of applicant skills, abilities, and experience; name, title, and office of evaluator), letters of recommendation by the first person in the chain of command, SARC, and the Senior Commander or the Commander; verification of assignment eligibility screening by the Commander or appointing authority; supervisor and commander statement of understanding, documentation of continuing education training courses; Department of Defense Sexual Assault Advocate Certification Program (D-SAACP) identification (ID) number.

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.

SARC and SAPR VAs may object to the collection of their PII by not submitting their PII on the required forms. However, they may not be considered qualified to perform their duties as a SARC and SAPR VA if they do not submit the information required to become certified.

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.

Applicants cannot give or withhold their consent to specific uses or their PII once submitted, however, PII will only be used for the purpose stated above and within the Privacy Act Statement.

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

DD 2950, Department of Defense Sexual Assault Advocate Certification Program (D-SAACP), Application Packet for New Applicants, and DD 2950-1, Department of Defense Sexual Assault Advocate Certification Program (D-SAACP), Renewal Application Packet

Authority: 10 U.S.C. 136, Under Secretary of Defense for Personnel and Readiness; and DoD Instruction 6495.03, Defense Sexual Assault Advocate Certification Program (D-SAACP).

Principal Purpose(s): The information provided on this form will be used to review and process applications for Sexual Assault Response Coordinator (SARC) and Sexual Assault Prevention and Response Victim Advocate (SAPR VA) certification.

Routine Use(s): To the Department of Justice Office for Victims of Crime and Training Technical Assistance Center for the purpose of verifying certified SARCs and SAPR VAs for participation in Advanced Military Sexual Assault Advocate Training. Additional routine uses may be found in the applicable system of notice DHRA 10, Defense Sexual Assault Advocate Certification Program at: <https://dpcl.d.defense.gov/Privacy/SORNsIndex/DoD-wide-SORN-Article-View/Article/570562/dhra-10-dod/>

Disclosure: Voluntary. However, if you are a SARC and SAPR VA and do not complete this form to become certified, you may be disqualified from the position. 10 U.S.C. 1561, note requires DoD to establish a certification program.

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

- | | | |
|--|----------|--|
| <input checked="" type="checkbox"/> Within the DoD Component | Specify. | Defense Manpower Data Center |
| <input checked="" type="checkbox"/> Other DoD Components | Specify. | Air Force, Army, Marine Corps, Navy and National Guard |
| <input checked="" type="checkbox"/> Other Federal Agencies | Specify. | Department of Justice- Office of Justice Programs, Office of Victims of Crimes |
| <input type="checkbox"/> State and Local Agencies | Specify. | |
| <input type="checkbox"/> 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. | |
| <input type="checkbox"/> 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 type="checkbox"/> Existing DoD Information Systems | <input type="checkbox"/> Commercial Systems |
| <input type="checkbox"/> Other Federal Information Systems | |

Individual

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 type="checkbox"/> Face-to-Face Contact | <input type="checkbox"/> Paper |
| <input type="checkbox"/> Fax | <input type="checkbox"/> Telephone Interview |
| <input 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 2950 and DD Form 2950-1

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.d.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.

I. 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. Cut off annually. Destroy 3 years after cutoff or 1 year upon employee separation or when superseded or obsolete, whichever comes first.

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. 36, Under Secretary of Defense for Personnel and Readiness; and DoD Instruction 6495.03, Defense Sexual Assault Advocate Certification Program (D-SAACP).

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.

This system does not collect information on members of the public. All SARC's and SAPR VAs are DoD civilians or Service members.

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 type="checkbox"/> Birth Date | <input type="checkbox"/> Child Information |
| <input type="checkbox"/> Citizenship | <input type="checkbox"/> Disability Information | <input type="checkbox"/> DoD ID Number |
| <input type="checkbox"/> Driver's License | <input checked="" type="checkbox"/> Education Information | <input type="checkbox"/> Emergency Contact |
| <input checked="" type="checkbox"/> Employment Information | <input type="checkbox"/> Financial Information | <input type="checkbox"/> Gender/Gender Identification |
| <input type="checkbox"/> Home/Cell Phone | <input type="checkbox"/> Law Enforcement Information | <input type="checkbox"/> Legal Status |
| <input type="checkbox"/> Mailing/Home Address | <input type="checkbox"/> Marital Status | <input type="checkbox"/> Medical Information |
| <input type="checkbox"/> Military Records | <input type="checkbox"/> Mother's Middle/Maiden Name | <input checked="" type="checkbox"/> Name(s) |
| <input checked="" type="checkbox"/> Official Duty Address | <input checked="" type="checkbox"/> Official Duty Telephone | <input checked="" type="checkbox"/> Other ID Number |
| <input type="checkbox"/> Passport Information | <input 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 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 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 | |

position type (Sexual Assault Response Coordinator (SARC) or Sexual Assault Prevention Representative Victim Advocate (SAPR VA)); Service/DoD affiliation and status; grade/rank; installation/command; work email address and telephone number; official military address of applicant and applicant's SARC (commanding officer, street, city, state, ZIP code, country); position level (Level I, II, III, or IV); certificates of training; date of application; verification of sexual assault victim advocacy experience (position, dates, hours, supervisor; name, title, and work telephone number of verifier); evaluation of sexual assault victim experience (description of applicant skills, abilities, and experience; name, title, and office of evaluator), letters of recommendation by the first person in the chain of command, SARC, and the Senior Commander or the Commander; supervisor and commander statement of understanding, documentation of continuing education training courses; Defense Sexual Assault Advocate Certification Program (D-SAACP) identification (ID) number.

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.

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

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

(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

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

Records are maintained in a controlled facility that employs physical restrictions such as double locks and is accessible only to authorized persons who hold key fobs. The data server is locked in a windowless room with restricted access. Additionally, all backups are physically stored in an off-site in a secure location. Paper files are stored in a locked filing cabinet in a locked room in the controlled facility.

(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

Access to electronic data files in the system is role-based, restricted to essential personnel only, and requires two factor authentication. All data is backed-up daily, encrypted, and stored on an encrypted hard drive.

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

- | | | |
|--|--|--|
| <input type="checkbox"/> Biometrics | <input type="checkbox"/> Common Access Card (CAC) | <input type="checkbox"/> DoD Public Key Infrastructure Certificates |
| <input checked="" type="checkbox"/> Encryption of Data at Rest | <input checked="" type="checkbox"/> Encryption of Data in Transit | <input type="checkbox"/> External Certificate Authority Certificates |
| <input type="checkbox"/> Firewall | <input type="checkbox"/> Intrusion Detection System (IDS) | <input type="checkbox"/> Least Privilege Access |
| <input type="checkbox"/> Role-Based Access Controls | <input type="checkbox"/> Used Only for Privileged (Elevated Roles) | <input checked="" type="checkbox"/> User Identification and Password |
| <input type="checkbox"/> Virtual Private Network (VPN) | <input checked="" type="checkbox"/> If Other, enter the information in the box below | |

Data is maintained in a secure database on encrypted servers. System access to case files is limited to computers within a closed network, not connected to the internet or other server.

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

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:

Liz Blanc Exceptional SARC Award

2. DOD COMPONENT NAME:

Defense Human Resources Activity

3. PIA APPROVAL DATE:

09/04/20

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.)

- From members of the general public 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
 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.

To collect, document, manage, and maintain awards data, from nomination to presentation, for DoD awards managed and maintained by the Defense Human Resources activity. The DoD Sexual Assault Prevention and Response Office (SAPRO) presents the Exceptional Sexual Assault Response Coordinator (SARC) Award each April to an individual (military or civilian) from each Military Service, the National Guard, and the Coast Guard. This award recognizes individuals whose work has been particularly noteworthy and demonstrates outstanding support of our Service members.

Information collected in the nominees includes: service title/rank, full name, installation name, work email, biography, and photograph.

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)

Mission-related uses

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.

Individuals are nominated by their Service Sexual Assault Prevention and Response Offices. Most information required for the nomination package is already held by the SAPR offices to facilitate mission activities. Individuals will be provided a Privacy Act Statement, however, when asked to provide additional information like a photograph.

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.

Individuals are nominated by their Service Sexual Assault Prevention and Response (SAPR) Offices. Most information required for the nomination package is already held by the SAPR offices to facilitate mission activities. Individuals, however, may elect for the SAPR offices not to nominate them when consulted.

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

AUTHORITY: 10 U.S.C. 136, Under Secretary of Defense for Personnel and Readiness; DoD Directive 5100.87, Department of Defense Human Resources Activity (DoDHRA); DoD Instruction 6495.02, Sexual Assault Prevention and Response (SAPR) Program Procedures

PURPOSE: To collect, document, manage, and maintain a data, from nomination to presentation, for the Liz Blanc Exceptional Sexual Assault Response Coordinator (SARC) Award.

ROUTINE USES: Disclosure of records are generally permitted under 5 U.S.C. 522a(b) of the Privacy Act of 1974, as amended. Routine uses are listed in the applicable System of Records Notice, DHRA 24, Defense Human Resource Activity Awards System currently pending publication.

DISCLOSURE: Voluntary, however, failure to provide requested information will inhibit nomination.

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.
- 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 Databases
- Existing DoD Information Systems Commercial Systems
- Other Federal Information Systems

Individuals, and SAPR Office leads and supervisors

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

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

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.d.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.

Submitted to DPCLTD on 7/22/2020

I. 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.

Cut off award packages annually, upon final determination (approved/disapproved) by calendar year. Destroy 15 year(s) 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; DoD Directive 5100.87, Department of Defense Human Resources Activity (DoDHRA); DoD Instruction 6495.02, Sexual Assault Prevention and Response (SAPR) Program Procedures

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.

This electronic collection does not collect information on members of the public.