

DOD PRIVACY IMPACT ASSESSMENT (PIA)

1. Department of Defense (DoD) Component:

DoD Office of the Undersecretary of Defense (Personnel and Readiness) Sexual Assault Prevention and Response Program Office (DoD/OUUSD/SAPRO).

2. Name of Information Technology (IT) System:

Defense Case Record Management System (DCRMS).

3. Budget System Identification Number (SNAP-IT Initiative Number):

Budget System Identification Number: 9990

4. System Identification Number(s) (IT Registry/Defense IT Portfolio Repository (DITPR)):

System Identification Number: 7506

5. IT Investment (OMB Circular A-11) Unique Identifier (if applicable):

Not Applicable.

6. Privacy Act System of Records Notice Identifier (if applicable):

A new Systems of Record Notice specific to DCRMS will be posted after DCRMS receives the ATO. This is per the OSD Policy Office – Identifier not available at this time.

7. OMB Information Collection Requirement Number (if applicable) and Expiration date:

Not applicable because this system only collects information from active military and DoD civilians, not the general public.

8. Type of authority to collect information (statutory or otherwise):

Statutory. Public Law 108-375 October 28, 2004; Section 577, Department of Defense Policy and Procedures on Prevention and Response to Sexual Assaults Involving Members of the Armed Forces. Also, 5 U.S.C. 301, Departmental Regulation, 10 U.S.C. 136, Under Secretary of Defense for Personnel and Readiness, E.O.9397 SSN), DoD Directive 6495.01, Sexual Assault Prevention and Response (SAPR) Program and DoDI 6495.02, Sexual Assault Prevention and Response (SAPR) Program Procedures.

9. Provide a brief summary or overview of the IT system (activity/purpose, present life-cycle phase, system owner, system boundaries and interconnections, location of system and components, and system backup):

Purpose: Enable DoD installations to comply with the requirements of DoD D 6495.01 Sexual Assault Prevention and Response (October 6, 2005).

Present life cycle phase: Staging Environment

System owner: DoD Washington Headquarters Services, Information Technology Management Directorate, WHS-Supported Organizations Division (DoD/WHS/ITMD/WSO)

System boundaries

The WSO network is separated and protected from the WHS Enterprise by a firewall. The WSO Helpdesk maintains all servers and network connections from the wall jack to the backbone connection. The backbone is maintained by the U.S. Army Information Technology Agency (ITA). The DCRMS server is located in the WSO Demilitarized Zone (DMZ). The DMZ has an external firewall allowing only minimally required port access to external users and an internal firewall allowing the same.

Firewalls and network intrusion detection system are deployed at the enclave boundary to the wide area network, at layered or internal enclave boundaries and at key points in the network, as required. Internet access is proxied through Internet access points that are physically or logically separated from other DoD information systems. Host-based intrusion detection systems are planned.

Remote access is permitted only for the system owners to make regular updates to the DCRMS software. This is accomplished via an encrypted CD that is sent on a regular basis (as updates are made) to WHS from the contractor (DefenseWeb).

Interconnections

10. Describe what information in identifiable form will be collected and the nature and source of the information (e.g., names, Social Security Numbers, gender, race, other component IT systems, IT systems from agencies outside DoD, etc.):

The Sexual Assault Response Coordinator collects case information from DoD military and civilian victims, and the military criminal investigation organization (MCIO), as needed. The information collected includes full name, last four digits of social security number (these two elements are only for Unrestricted Reports, which are not confidential and are processed through the investigative/legal system), gender, ethnicity, date-of-birth, marital status, military status, and MCIO case number. In some instances, the Victim Advocate may enter data into DCRMS, but the SARC will review all data.

11. Describe how the information will be collected (e.g. via the Web, via paper based collection, etc.):

The Sexual Assault Response Coordinator (SARC) or Victim Advocate (VA) collects the information outlined above and enters it in this system via Web-based interface.

12. Describe the requirement and why the information in identifiable form is to be collected (e.g., to discharge a statutory mandate, to execute a Component program, etc.):

Statutory. Public Law 108-375 October 28, 2004; Section 577, Department of Defense Policy and Procedures on Prevention and Response to Sexual Assaults Involving Members of the Armed Forces. Also, 5 U.S.C. 301, Departmental Regulation, 10 U.S.C. 136, Under Secretary of Defense for Personnel and Readiness, E.O.9397 SSN), DoD Directive 6495.01, Sexual Assault Prevention and Response (SAPR) Program and DoDI 6495.02, Sexual Assault Prevention and Response (SAPR) Program Procedures.

13. Describe how the information in identifiable form will be used (e.g., to verify existing data, etc.):

The SARC manages the case file of the sexual assault victims, coordinating care and services to assist the victim. To facilitate their case management, the SARCs need a system that tracks services a victim is entitled to and has received, individuals involved in a particular case (law enforcement, counselors, legal, etc) - so the SARC can be sure the victim is receiving all the services they are eligible to receive.

14. Describe whether the system derives or creates new data about individuals through aggregation (collective parts):

The system holds basic demographics and support services that were provided to the victim. This is not a medical record under HIPAA protection. The system holds the investigative case number, basic demographics on the victim, what services they have been referred to (e.g. counseling, medical, etc), but no details of the medical or counseling visits. The information stored in DCRMS is very general, and not detailed. If subpoenaed it would provide little information, and would not provide additional information to that stored in other systems such as law enforcement or medical data systems. There is no plan at this time to aggregate data fields.

15. Describe with whom the information in identifiable form will be shared, both within the Component and outside the Component (e.g., the other DoD Components, Federal agencies, etc.):

Identifiable information will be available only to the Sexual Assault Response Coordinators or Victim Advocates (depending on the Service) and will not be shared with any other individuals or agencies.

16. Describe any opportunities individuals will have to object to the collection of information in identifiable form about themselves or to consent to the specific uses of the information in identifiable form. Where consent is to be obtained, describe the process regarding how the individual is to grant consent:

Victims have the option of filing a Restricted Report, which is confidential and does not contain personal identifying information on any document. If the victim does not want the case to go forward to law enforcement or the commander, they can choose this option. If they choose an Unrestricted Report, they are made aware that their identifying information will not be confidential and will be entered through the system. It is necessary for the SARC to enter the identifying information so that the SARC can track services provided to that victim. The SARC is part of the treatment/case process and just as the victim must provide identifying information to health care providers and law enforcement, they will have to provide their identifying information to the SARC.

Individuals seeking access to their case information contained in this system of records should address written requests to Director, Sexual Assault Prevention and Response Office, 1401 Wilson Blvd, Suite 402, Arlington, VA 22209-2318. Requests should contain the full names of the individual, last four digits of the individual's Social Security Number, individual's service, individual's date of birth, sex, treatment facility(ies) that have provided care, and fiscal year(s) of interest. OSD rules for accessing records, for contesting contents and appealing initial agency determinations are contained in OSD Administrative Instruction 81; 32 CFR part 311; or may be obtained from the system manager. The Director of SAPRO will work with the Service SAPR office of the requesting individual to insure they receive their data in DCRMS

17. Describe any information that is provided to an individual, and the format of such information (Privacy Act Statement, Privacy Advisory) as well as the means of delivery (e.g., written, electronic, etc.), regarding the determination to collect the information in identifiable form:

The SARC must inform the victim of the Privacy Act, what data is being entered, and uses of those data. To insure that this happens, when the SARC begins to enter a new case, a window will pop-up with the Privacy Act Word document for the SARC to print and give to/discuss with the victim. This document will be automatically dated.

PRINCIPAL PURPOSES: To provide a DoD-wide system to facilitate the case management of victims of sexual assault by the SARC. Case management includes tracking the services a victim is entitled to and has received, individuals involved in a particular case (law enforcement, counselors, legal, etc.) so the SARC can ensure a

victim is receiving all services for which eligible. This system will also assist the Military Services in complying with statutory and regulatory reporting requirements on victim service provision and restricted reports. Demographic data, with personal identifiers removed, can be included in reports used by agency officials and employees, or authorized contractors, and other DoD Components to manage programs and answer programmatic questions.

DCRMS web usage data will be used to validate continued need for user access to DCRMS databases, to address problems associated with web access, and to ensure that access is only for official purposes. This is part of the security process.

Routine uses of records maintained in the system, including categories of users and the purposes of such uses:

In addition to those disclosures generally permitted under 5 U.S.C. 522a(b) of the Privacy Act, these records or information contained therein may specifically be disclosed outside the DoD as a routine use pursuant to 5 U.S.C. 522a(b)(3) as follows:

The DoD 'Blanket Routine Uses' set forth at the beginning of OSD's compilation of systems of records notices apply to this system – with the stipulation that only aggregate level data with no personal identifying information included be made available.

Disclosure: Voluntary. However, if the individual declines to provide the information requested, SARC, victim advocates, and SA program managers will not be able to efficiently and effectively ensure case resolution for each victim's sexual assault complaint.

18. Describe the administrative/business, physical, and technical processes and controls adopted to secure, protect, and preserve the confidentiality of the information in identifiable form:

A comprehensive set of security control mechanisms and procedures is currently active within the WSO Network Operations Center supporting DCRMS. The set of controls are summarized below:

Personnel Access. Access to the development facility and networks is monitored and controlled at all times.

Automated Data Processing (IT) Position Sensitivity Designations. All individuals that have access to the DCRMS development or production systems, must have obtained or have applied for at least an ADP II (IT Level II) position sensitivity designation.

Account Security. Each individual authorized to use a networked computing system must have a unique user-id and password, and users are not permitted to share passwords.

Computer Room. Access is restricted to authorized individuals with appropriate badges or escorted individuals. A visitor log is maintained.

Emergency Procedures. The WSODD staff is briefed on shutdown procedures to safeguard DCRMS data in the event of an emergency situation.

Material Control. All incoming materials and supplies are subject to inspection. Removal of materials must be approved in advance. The IT Department Staff performs anti-virus checks of all magnetic media prior to using it on facility equipment

Video Terminals and Workstations. All networked computing systems remain in locked and protected areas to prohibit access or observance by unauthorized individuals. Screen savers (or other access control mechanisms) with password protection are employed.

Any media containing Sensitive Information, Protected Health Information, or information protected by the Privacy Act of 1974 (SI/PHI/PAD) that is to leave the designated work area is encrypted and securely wrapped and labeled to indicate the data's sensitivity. When no longer needed, SI/PHI/PAD data is properly destroyed. In the event that such data is inadvertently disclosed, the DCRMS Project Management contacts the Customer Automated Information System Security Program Office and the OSC/JS Privacy Office immediately upon discovery of disclosure.

19. Identify whether the IT system or collection of information will require a System of Records notice as defined by the Privacy Act of 1974 and as implemented by DoD Directive 5400.11, "DoD Privacy Program," November 11, 2004. If so, and a System Notice has been published in the Federal Register, the Privacy Act System of Records Identifier must be listed in question 6 above. If not yet published, state when publication of the Notice will occur;

Yes, immediately after the ATO is granted the SORN will be submitted to the OSD Privacy Office.

20. Describe/evaluate any potential privacy risks regarding the collection, use, and sharing of the information in identifiable form. Describe/evaluate any privacy risks in providing individuals an opportunity to object/consent or in notifying individuals. Describe/evaluate further any risks posed by the adopted security measures:

For Unrestricted Reports (UR) of sexual assault involving military members (in this case, victims), the Sexual Assault Response Coordinator (SARC) manages the case file for the victim – coordinating referrals and visits to health care, counseling, with investigators and legal – identifying information is necessary for tracking services and not an optional data field For the URs, the victim's identifying information (SSN) is in many database

systems in its entirety, in DCRMS it is the only the last four, with provides a better level of security. For the victim to receive services from the SARC, the SARC will need the identifying information. For Restricted Reports, which are confidential, there is no identifying information on the victim entered into DCRMS.

The SARCs/VAs are screened by the Services and access to PI is only at that level – SAPR programs and managers, as well as DoD, receive no personally identifiable information. SARCs/VAs have strong passwords and the Website will be monitored by DoD/WHS/TTMD/WFO for attempts to exploit or find system vulnerabilities and to be sure there are no security breaches.

All information is covered by the Privacy Act.

21. State classification of information/system and whether the PIA should be published or not. If not, provide rationale. If a PIA is planned for publication, state whether will be published in full or summary form:

The data collected is unclassified, but will be marked and only used For Official Use Only (FOUO). Full PIA will be published.