

## SUPPORTING STATEMENT (Refer to OMB Form 83-I INST)

### A. JUSTIFICATION

#### 1. Need for the Information Collection

Section 563 of Public Law (PL) 110-417, the National Defense Authorization Act (NDAA) for Fiscal Year (FY) 2009, directs the Secretary of Defense to implement a centralized case-level database for the collection and maintenance of information regarding sexual assaults involving members of the Armed Forces, including information, if available, about the nature of the assault, victim, offender, and case outcomes in connection with the assault. Specifically, the system will collect data regarding incidences of sexual assault involving persons covered by DoD Directive (DoDD) 6495.01. Those individuals are as follows:

- a. National Guard and Reserve Component members who are sexually assaulted when performing active service, as defined in section 101(d)(3), Chapter 47 of Title 10, United States Code (U.S.C.), and inactive duty training;
- b. Military dependents 18 years of age and older, who are eligible for treatment in the military healthcare system, at installations in the continental United States (CONUS) and outside of the continental United States (OCONUS), and who were victims of sexual assault perpetrated by someone other than a spouse or intimate partner;
- c. The following non-military personnel;
  - i. DoD civilian employees and their family dependents 18 years of age and older when they are stationed or performing duties OCONUS and eligible for treatment in the military healthcare system at military installations or facilities OCONUS;
  - ii. U.S. citizen DoD contractor personnel when they are authorized to accompany the Armed Forces in a contingency operation OCONUS and their U.S. citizen employees per DoDI 3020.41.
- d. Service members who are on active duty but were victims of sexual assault prior to enlistment or commissioning.

The system will also collect data regarding incidences of sexual assault involving National Guard and Reserve Component members, as defined in Title 32, U.S.C. in accordance with Memorandum Subject: National Guard Sexual Assault Prevention and Response (SAPR) Program Policy Guidance, dated September 1, 2010.

The system will include the capability for capturing data via manual entry or automated system interfaces; generating various level reports and queries; and conducting case and business management. At the Military Service level, Sexual Assault Response Coordinators (SARC) and Sexual Assault Prevention and Response (SAPR) Victim Advocates (VA) 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 data is used to respond to mandated reporting requirements.

## 2. Use of the Information

When implemented, the Defense Sexual Assault Incident Database (DSAID) will have the following primary functions:

- a. Enhance the transparency of sexual assault-related data, while adhering to the privacy and Restricted Reporting options for sexual assault victims;
- b. Provide accurate and timely ad-hoc query and reporting of sexual assault incidents to meet congressional requirements;
- c. Enable SARC to input and maintain sexual assault cases; and
- d. Allow for business management in support of SAPR program manager administration and case management.

DSAID will also enhance data analysis and trend identification capabilities and allow for evaluation of Sexual Assault Prevention and Response Office (SAPRO) and Military Service SAPR programs.

At the local level, SARCs and SAPR VAs will work with victims to ensure they are aware of reporting options and services available, and then connect them with appropriate resources, including medical care, mental healthcare, legal advice, and spiritual support. At the DoD level, only de-identified data is used to respond to mandated reporting requirements. SAPRO has access to identified closed case information and de-identified, aggregate open case information for study, research, and analysis purposes.

## 3. Use of Information Technology

Case information maintained in DSAID will be received, when appropriate, from Military Service-specific systems that capture sexual assault data to include Military Criminal Investigative Organizations' (MCIO) and Offices of the Judge Advocate General (OTJAG) systems.

SAPRO, the U.S. Army, the U.S. Marine Corps, the U.S. Navy, the U.S. Air Force, and the National Guard Bureau SAPR program managers as well as SARCs at the installation and command levels will have the ability to access DSAID.

SAPRO will use DSAID to generate congressionally mandated Annual and Military Service Academy reports; quarterly reports; run ad-hoc queries; track sexual assault victim support services; support SAPR program administration and reporting requirements; control user access assignment of DSAID for Service SAPR program managers; and perform data analysis.

Military Service SAPR program managers will control DSAID user access assignments within their respective Military Service, including SARC assignments that support joint operations; track the life cycle of a sexual assault case; and support SAPR program administration and program reporting requirements. Military Service system managers will assist the Military Service SAPR program manager to maintain SARC profiles as well as run their respective Military Service level reports and ad hoc queries.

SARCs will contribute both Restricted and Unrestricted data; track the life cycle of the sexual assault case; support SAPR program administration; and maintain SAPR VAs profiles.

If a victim of a sexual assault involving a member of the Armed Forces chooses the Restricted Reporting option, no personally identifiable information (PII) is collected. If an Unrestricted Report is made, the victim voluntarily provides requested PII, and the matter is referred to law enforcement for investigation.

#### **4. Non-duplication**

Presently, each Military Service maintains a number of systems that support the various communities involved in providing support to victims of sexual assault and other response elements to include criminal investigative and legal communities. A system to consolidate and centralize this data does not exist, which makes cradle-to-grave case management, reporting, accurate trend analysis on the efficiency of training programs, and victim care difficult and labor intensive. The current service systems and status are as follows:

- a. The Department of the Army's Sexual Assault Data Management System (SADMS) is currently deployed and captures victim, subject, incident, and investigative information.
- b. The Department of the Army's Sexual Harassment/Assault Response and Prevention (SHARP) is currently in development and captures victim, subject, incident, and investigative information. Once deployed, SHARP will supersede SADMS.
- c. The Department of the Navy's Consolidated Law Enforcement Operations Center is currently deployed and captures investigative and legal information.
- d. The Department of the Navy's Sexual Assault Victim Intervention Case Management System is currently deployed and captures victim, incident and subject information.
- e. The Marine Corps' Sexual Assault Incident Reporting Database is currently deployed and captures victim and incident (Restricted Reporting only) information.
- f. The Department of the Air Force's Investigative Information Management System is currently deployed and captures case investigative information.

These sources of data have been examined, and they do not meet the mandate as they are Military Service specific and not DoD-wide systems. Additionally, they lack the

capability to run reports that meet current congressional and Departmental reporting requirements.

#### 5. Burden on Small Business

DSAID will not collect or maintain information related to small businesses or other small entities.

#### 6. Less Frequent Collection

At this time, it is estimated that DSAID will be required to generate roughly 21 standard Military Service and Military Service Academy reports a year. They are generated by DSAID either quarterly or annually. Two of these standard reports are congressionally mandated. The system will also produce weekly ad hoc queries and reports, as well as respond to congressional and Government Accountability Office (GAO) inquiries as needed.

There would be no consequences if the collection were conducted less frequently.

#### 7. Paperwork Reduction Act Guidelines

There are no special circumstances that require the collection of information for DSAID to be conducted in a manner inconsistent with the guidelines delineated in 5 Code of Federal Regulations (CFR) 1320.5(d)(2).

#### 8. Consultation and Public Comments

a. Public comments were solicited in the preamble of the interim final rule (77 FR 4239). No comments were received.

b. The Privacy Act System of Records Notice (SORN), DHRA 06 DOD, "Defense Sexual Assault Incident Database," was initially published on December 15, 2009 (74 FR 66298). A SORN alteration was published June 20, 2012 (77 FR 37002). A Privacy Impact Assessment was initially completed in September 2009 and was updated in May 2012.

c. Section 563 of PL 110-417, the NDAA for FY09, directed the implementation of DSAID. A working group was established in early 2008 to design a system that will be useful and relevant to the needs of the Department and each Military Service. It consisted of representation from SAPRO, each of the Military Services, the National Guard Bureau, the Office of the Assistant Secretary of Defense (OASD) for Reserve Affairs (RA), OASD for Health Affairs (HA), and the Joint Chiefs of Staff (JCS). Together, the working group created a high level design concept document for DSAID. The group submitted a proposal to the Department, which it accepted and delivered to the Congress in 2009. SAPRO further collaborated with the stakeholders from each of the Military Services and established a more detailed DSAID requirements package that was used as the basis for a contract to develop the system. SAPRO is currently working with the developer to design, test and implement DSAID in

preparation for the initial operating capability. Further enhancements and upgrades to DSAID will be evaluated and approved by the DSAID Change Control Board (CCB).

The Department will continue to work with the Military Services and other stakeholders regarding the availability of requested information, frequency of collection, and clarity of instructions to further develop DSAID. Consultations with stakeholders is planned to occur on a monthly basis through the DSAID CCB process.

#### 9. Gifts or Payment

Gifts or payments will not be provided to respondents. However, victims and alleged perpetrators may be entitled for benefits allowed by the law.

#### 10. Confidentiality

DSAID will collect victim and alleged perpetrator personal identifiers, incident information, and case outcomes in connection with the assault. PII is collected by SARCs and sometimes SAPR VAs. The collection of case information will be used to document elements of the sexual assault reporting process and comply with the procedures in place to effectively manage the Department's SAPR programs. In order to safeguard individual privacy, case information is 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 is role based and requires the use of a Common Access Card. Further, at the DoD level, only de-identified data can be accessed.

DSAID will reside on the Pentagon network. The protections on the network will include firewalls, passwords, and web-common security architecture. Access roles and permission lists for SAPRO personnel and SARCs are granted by SAPR program managers through the assignment of appropriate user roles. No other personnel other than those with role-based access can have access to an individual's PII unless permission is granted from the individual in writing to release the information.

These For Official Use Only records are 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."

Details regarding the steps taken to ensure PII confidentiality are articulated in DHRA 06 DoD and the "Privacy Impact Assessment (PIA) for the Defense Sexual Assault Incident Database." A copy of the SORN and the PIA are located in this information collection package.

## **11. Sensitive Questions**

As stated, victims of sexual assault have two options when reporting information regarding an incident. Victims may consent to a full collection of information, which will initiate an investigation through the election of the Unrestricted Reporting option; or they may report in a way that enables them to receive assistance without initiating an investigation through the election of a Restricted Report. If a victim elects the Restricted Reporting option, no PII will be collected but full or limited SAPR services may be available. Alleged perpetrator PII in case of an Unrestricted Reporting is collected by Military Service MCIO systems and is loaded into DSAID after reasonable suspicion has been found that the alleged perpetrator may have committed the crime. In this way, no collected information violates the Privacy Act, as implemented by DoD 5400.11-R.

## **12. Respondent Burden, and its Labor Costs**

### **a. Estimation of Respondent Burden**

The Department reports an average of 3,200 incidents of sexual assault involving a Service member each year. It estimated that it takes the respondent approximately 1 hour to provide information.

As discussed, information collected in DSAID will come from several sources. These sources include Military Service-specific MCIO systems and input from SARCs who will contribute both Restricted and Unrestricted Reporting data.

The total annual hours requested reported in Item 13, of OMB Form 83-I, is 3,200 hours.

### **b. Labor Cost of Respondent Burden**

The estimated annualized cost to respondents of the burden hours imposed by the collection is \$23,200 (3,200 x \$7.25).<sup>1</sup> This does not include capital, start-up, contracting out, or operations and maintenance costs. Respondent cost other than burden hour costs are shown in Item 13 of this Supporting Statement.

## **13. Respondent Costs Other Than Burden Hour Costs**

The estimated annualized costs to respondents, other than the burden hour costs addressed in Item 12, resulting from the collection of information is as follows:

a. Total capital and start-up costs annualized over the expected useful life of the item(s) is \$0.00. Total operation and maintenance costs to respondents is \$0.00.

## **14. Cost to the Federal Government**

---

<sup>1</sup> Department estimate is based on the federal minimum wage, which, as of September 2011, is \$7.25.

Please reference the following Rough Order of Magnitude (ROM) Basis of Estimate:

Major Implementation Cost Component	Estimated CMS Alternative Cost	Extended Cost Estimate	Notes
1. COTS CMS Licenses	\$10,000	\$2,000,000	Estimated cost of 200 concurrent user licenses – exact cost will only be determined during final development stage since fees are proportional to the amount of hardware processor capability
2.0 COTS Configuration 2.1 COTS CMS Software Configuring (Code)	-	\$2,537,000	Estimated code development costs for all configuration needs
2.2 Processing Customization Code	\$1,000,000	\$1,000,000	Analysis processing capability development
2.3 Interface Configuration Code	\$900,000	\$5,400,000	Average interface for all six service source systems which includes the code to develop a common data exchange format code and cross walk algorithm of service specific to SAPR data element relationship mapping
2.4 Glue Type Code Customization	\$700,000	\$700,000	Development code required to glue customization to base code capabilities
2.5 Reporting Code Customization	\$500,000	\$500,000	Development code estimate for standardized trend analysis reports
3. Hardware	\$30,000	\$30,000	Servers and network peripherals along with source system peripherals
4. Hardware & Software Deployment	\$7,000	\$7,000	Software installation and hardware settings to achieve a basic installed functionality with all sources and components
5. User Acceptance Testing	\$500,000	\$500,000	User acceptance testing will require iterative modifications due to inevitable interface changes despite a change management freeze on service source interface configurations as well as validation of use case scenarios

*Total Estimated Cost:*      \$12,674,000

*+/- 45% uncertainty tolerance - primarily due to limited definition of configuration and interface complexity*

## 15. Reasons for Change in Burden

The reason for the change in burden, as indicated in Item 13 of OMB Form 83-I, is due to a program change mandated by Section 563 of PL No. 110-417, the NDAA for FY09.

**16. Publication of Results**

Aggregate data collected in DSAID will be published in accordance with Section 577(f) of PL No. 108-375, the NDAA for FY05. Section 596 of PL No. 109-163, the NDAA for FY06, and Section 583 of PL No. 109-364, the NDAA for FY07, impose additional requirements for the report. The mandate requires the collection of sexual assault information involving members of the Armed Forces annually and that the publication of this data be submitted to Congress.

In order to protect individual privacy, personal descriptors, such as PII, will not be published. Data that is published will remain in numerical form.

**17. Non-Display of OMB Expiration Date**

DSAID will display of the expiration date of OMB approval on the entry page.

**18. Exceptions to “Certification for Paperwork Reduction Submissions”**

There is no provision of Item 19.a of OMB Form 83-I which cannot be certified.

**B. COLLECTIONS OF INFORMATION EMPLOYING STATISTICAL METHODS**

The collection of information in DSAID does not employ statistical methods, as indicated in Item 17 of OMB Form 83-I.