Privacy Impact Assessment
for the

Defense Sexual Assault Incident Database (DSAID)

DHS/USCG/PIA-028

June 10, 2019

Contact Point
Shawn Blaine/Andrea Mckie
SAPR PROGRAM CG-1111
U.S. Coast Guard
(202) 475-5151

Reviewing Official
Jonathan R. Cantor
Acting Chief Privacy Officer
Department of Homeland Security
(202) 343-1717

Abstract

The Department of Defense (DoD) owns and operates the Defense Sexual Assault Incident Database (DSAID) system, which serves as a centralized, case-level database for military sexual assault reports. DSAID is a case management and business management tool that contains information provided by all military services, and provides information that can be used to build metrics and track cases from start to conclusion. The United States Coast Guard (USCG) is conducting this Privacy Impact Assessment (PIA) because the DSAID system collects and maintains personally identifiable information (PII) about USCG personnel and other individuals involved in cases.

Overview

Section 563 of Public Law 110-417[1] required DoD to create and use a single system for tracking reports of sexual assault. DSAID is the system adopted by DoD.[2] Although the requirement to create a specific database applied only to DoD, the USCG provides information to DoD for inclusion in the DoD Annual Report on Sexual Assault in the Armed Forces, and the USCG has its own legal requirement for a service-specific annual report on sexual assault.[3] Thus, the use of DSAID to track reports of sexual assault in the USCG was necessary in order to ensure that the USCG was tracking the same information about sexual assaults and in the same way as the other Armed Forces.

Additionally, the John Warner National Defense Authorization Act, Section 532 of Public Law 109-364,[4] requires an annual report on the effectiveness of the policies, training, and procedures of each Military Service Academy for sexual harassment and violence for Academy personnel. Federal law also requires the DoD to provide Congress with an annual report on sexual assaults involving members of the Armed Forces. This report involves numerical data and statistics drawn from metrics identified in DoD's evaluation plan. It satisfies the Ike Skelton National Defense Authorization Act for Fiscal Year 2011, Public Law 111-383,[5] requirement regarding improvement to the sexual assault prevention and the response program.

The USCG has long recognized the importance of a strong Sexual Assault Prevention and Response (SAPR) Program, and has taken direct actions, such as hiring a dedicated Program Manager and chartering a Task Force to examine sexual assault training, policy, investigations, communications, and culture, to address the problem. In January 2013, these efforts culminated

[1] *See* https://www.gpo.gov/fdsys/pkg/PLAW-110publ417/html/PLAW-110publ417.htm.
[2] For more information, please *see* Privacy Impact Assessment: (PIA) Defense Sexual Assault Incident Database (DSAID), *available at* http://www.dhra.mil/Portals/52/Documents/Privacy/PIA/DSAID_DHRA%2006_PIA_20180702.pdf.
[3] Section 217 of Public Law 111-281. *See* https://www.congress.gov/111/plaws/publ281/PLAW-111publ281.pdf.
[4] *See* https://www.gpo.gov/fdsys/pkg/PLAW-109publ364/html/PLAW-109publ364.htm.
[5] *See* https://www.gpo.gov/fdsys/pkg/PLAW-111publ383/html/PLAW-111publ383.htm.

with the Coast Guard's establishment of the Sexual Assault Prevention Council as a cross-directorate body comprised of shareholders in the SAPR Program and processes.

The USCG goal is to prevent sexual assault through efforts that influence the knowledge, skills, and behaviors of all members, and stop sexual assault before it occurs. The USCG mission is to eliminate sexual assault from the service, and ensure that if it does occur, to provide immediate victim support; a responsive and intimidation-free reporting environment; timely, professional investigations; and accountability for those who commit this crime or who stand by and allow it to occur.

With the help of the SAPR Program, the USCG seeks to eliminate sexual assault by implementing and sustaining comprehensive SAPR strategies that focus on prevention, including awareness and cultural change.

Sexual Assault Response Coordinators (SARC) use DSAID as their primary case management tool for working with sexual assault victims. This database functions to assist in monitoring the services offered to care for victims, such as to counseling referrals and referrals to a chaplain. DSAID records information about the actual assault, and also provides information about the recovery efforts SARCs manage.

When a sexual assault case has been made, a report comes to the SARC or Victim Advocate. The SARC makes contact with the victim and arranges a meeting to explain the process of making a report and the reporting options to the victim. The SARC explains to the victim that he or she will be asked questions to establish a case and the information obtained will be placed in a database. The victim makes a reporting option selection (i.e., unrestricted,[6] restricted[7]) and signs the Victim Reporting Preference Statement form (CG-6095). The SARC will also document additional information from the victim on the DSAID Data Form (DD Form 2965). The SARC will upload the CG-6095 into DSAID, and transfer the information from DD Form 2965 into DSAID. DD Form 2965 is shredded after the information is entered into DSAID and CG-6095 is

[6] **Unrestricted Reporting** involves a service member or adult armed forces dependent who is sexually assaulted and desires medical treatment, counseling, and an official investigation of his or her allegation. He or she can report the matter using official reporting channels (e.g., duty watch stander, supervisor, the chain of command, local authorities). The Unrestricted Reporting option provides for an immediate formal investigation by trained criminal investigators, as well as the full range of protections to the victim including immediate transfer or relocation, an expedited transfer, and other police and command protective actions, if necessary. It is the only option that may lead to offenders being held accountable for their actions.

[7] **Restricted Reporting** is a confidential report to authorized individuals (SARC, Victim Advocate, or Coast Guard/DoD health care provider) to receive advocacy, legal counsel, medical treatment, or counseling. This report does not trigger an official investigation or command notification. Exceptions to Restricted Reporting do exist and the option can be taken away for various situations, such as a safety risk. More information can be found in the Department of Defense Instruction DODI 6495.02 Sexual Assault Prevention and Response, *available at* http://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/649502p.pdf.

placed in a double-locked file in the applicable SARC's office. The SAPR Program Office (CG-1111) has oversight of the SARCs' use of DSAID.[8]

Additionally, DSAID supports Military Service SAPR program management and DoD Sexual Assault Prevention & Response Office oversight activities. DSAID serves as the DoD's SAPR source for internal and external requests for statistical data on sexual assault in accordance with Section 563 of Public Law 110-417. DSAID assists with annual and quarterly reporting requirements, identifying and managing trends, analyzing risk factors or problematic circumstances, and taking action or making plans to eliminate or mitigate risks. DSAID gives SARCs the enhanced ability to provide comprehensive and standardized victim case management. DSAID receives information from the Military services' existing data systems or by direct entry by authorized Military Service Personnel, such as USCG personnel.

DSAID contains unrestricted and restricted military sexual assault reports and includes safeguards to shield PII from unauthorized disclosure. Unrestricted reports will be investigated by law enforcement, whereas restricted reports will not prompt an investigation and the report will be made only to a SARC or a Victim Advocate. No criminal case will be opened. DSAID will not contain PII of victims who make a restricted report.

Section 1.0 Authorities and Other Requirements

1.1 What specific legal authorities and/or agreements permit and define the collection of information by the project in question?

The Coast Guard is authorized to collect this information and conduct this mission under Section 217 of Public Law 111-281; Section 532 of Public Law 109-364; Section 563 of Public Law 110-417; the John Warner National Defense Authorization Act; and the Ike Skelton National Defense Authorization Act for Fiscal Year 2011, Public Law 111-383.

1.2 What Privacy Act System of Records Notice(s) (SORN(s)) apply to the information?

DHS/USCG-002 Employee Assistance Program (EAP) Records,[9] which is being updated concurrently with the completion of this PIA.

[8] DSAID is not an investigative database. This system functions as a case management tool to monitor the care provided to assist victims; however, it is not part of the legal process. Only demographic information of the subject and outcome information is added when provided by Coast Guard Investigative Service (CGIS) and/or legal.
[9] The previous USCG EAP SORN can be found at 79 FR 74736 (December 16, 2014).

1.3 Has a system security plan been completed for the information system(s) supporting the project?

Yes. The Office of the Secretary of Defense (OSD) Nonsecure Internet Protocol Router (NIPR) OSD NIPRNet System Security Plan v1.8 has been completed.

The Authority to Operate (ATO) for DSAID expires August 2, 2019.

1.4 Does a records retention schedule approved by the National Archives and Records Administration (NARA) exist?

Yes. DSAID replaced the previous DoD system, Defense Case Records Management System (DCRMS), which was scheduled under DAA-0330-2013-0005, stating DSAID cutoff cases at the end of the fiscal year; the retention period is 50 years after cutoff.

1.5 If the information is covered by the Paperwork Reduction Act (PRA), provide the OMB Control number and the agency number for the collection. If there are multiple forms, include a list in an appendix.

OMB Control Number 0704-0482, Defense Sexual Assault Incident Reporting. CG Form-6095 is still undergoing the PRA process to be assigned an OMB Control number.

Section 2.0 Characterization of the Information

2.1 Identify the information the project collects, uses, disseminates, or maintains.

DSAID maintains the following information from members of the general public and USCG active duty, reserve, retired active duty, and reserve military personnel and their eligible dependents.[10]

Victim Information for Unrestricted Reports

- Name;
- Defense Sexual Assault Incident Database (DSAID) control number (i.e., system-generated unique control number);
- Social Security number;

[10] Eligible dependents are those 18 years or older. The sexual assault must not be a family advocacy case in which the parties involved are intimate partners and/or members within the same family.

- Passport number;
- U.S. permanent residence card or foreign identification;
- Date of birth;
- Address;
- Phone number;
- Duty Station;
- Age;
- Race;
- Ethnicity; and
- Rank/grade.

Alleged Perpetrator Information for Unrestricted Reports

- Name;
- Defense Sexual Assault Incident Database (DSAID) control number (i.e., system-generated unique control number);
- Social Security number;
- Passport number;
- U.S. permanent residence card or foreign identification;
- Date of birth;
- Address;
- Phone number;
- Duty Station;
- Age;
- Race;
- Ethnicity; and
- Rank/grade.

Victim Information for Restricted Reports

If a victim of a sexual assault involving a member of the Armed Forces makes a restricted report (i.e., a report that does not initiate an investigation) of sexual assault, no PII for the victim or alleged perpetrator is maintained in DSAID. Any PII collected is stored in a double-locked file and maintained at the local command.

2.2 What are the sources of the information and how is the information collected for the project?

DSAID data is collected by the SARC directly from the victim. The information is initially documented on DD Form 2965 and then transferred into the database. CG-6095, which collects the victim's reporting option selection, is uploaded into the database as well. DD Form 2965 is shredded after the information has been entered into the database and CG-6095 is kept in a double-locked file.

DSAID receives information directly from victims of sexual assault via SARCs. Only authorized sexual assault program managers and military service legal offices have access to DSAID.

2.3 Does the project use information from commercial sources or publicly available data? If so, explain why and how this information is used.

DSAID does not use or correlate information from commercial or publicly available sources.

2.4 Discuss how accuracy of the data is ensured.

DSAID receives data from SARCs, who receive it directly from the victim and is validated upon receipt.

2.5 Privacy Impact Analysis: Related to Characterization of the Information

Privacy Risk: There is risk that information manually entered into the database could be entered incorrectly by SARCs.

Mitigation: This risk is mitigated. A quality assurance process is in place to review information in the database for completeness and accuracy. A monthly report is provided to each SARC Regional Manager regarding the status of the information being maintained on cases within his or her jurisdiction. The SARC will be contacted by the SAPR Field Coordinator to address any issues noted on their individual cases.

Privacy Risk: There is a risk that the information collected from the victims could be inaccurate.

Mitigation: This risk cannot be fully mitigated. However, all authorized USCG users are trained by the DoD Sexual Assault Prevention & Response Office, and also complete an online training course to ensure accurate reporting standards. Victims of sexual assault have two options when reporting information regarding an incident. Individuals may either consent to a full collection of information by making an Unrestricted Report, which will initiate legal proceedings, or they may make a Restricted Report that enables them to receive assistance without legal obligation. If a victim of a sexual assault involving a member of the Armed Forces makes a Restricted Report of sexual assault, no victim or alleged perpetrator PII is entered into DSAID.

Section 3.0 Uses of the Information

3.1 Describe how and why the project uses the information.

The USCG policy for the SAPR Program (COMDTINST M1754.10E)[11] mandates the collection of information for every report of sexual assault. The DSAID system is used to centralize case-level sexual assault data involving a member of the Armed Forces, in a manner consistent with DoD and USCG regulations for Unrestricted and Restricted reporting. This includes information, if available, about the nature of the assault (e.g., incident date and location, type of offense), the victim, the alleged perpetrator, case outcomes in connection with the assault, and other information necessary to fulfill reporting requirements. Records may also be used as a management tool for statistical analysis tracking, reporting, evaluation program effectiveness, and conducting research.

USCG and other armed services' SAPR Programs will use DSAID to track military sexual assaults and assess the effectiveness of response efforts. Furthermore, the USCG will use DSAID to standardize reporting requirements and ensure transparency of sexual assault-related data.

3.2 Does the project use technology to conduct electronic searches, queries, or analyses in an electronic database to discover or locate a predictive pattern or an anomaly? If so, state how DHS plans to use such results.

No, DSAID does not use technology to conduct electronic searches, queries, or analyses to discover or locate a predictive pattern or an anomaly.

[11] *See* https://media.defense.gov/2017/Mar/29/2001723560/-1/-1/0/CIM_1754_10E.PDF.

3.3 Are there other components with assigned roles and responsibilities within the system?

No, other DHS Components do not have access to DSAID. Additionally, only those with system administrator access have access to USCG data. For example, another Department of the Armed Forces would not have access to USCG information.

3.4 Privacy Impact Analysis: Related to the Uses of Information

Privacy Risk: There is a risk that information in a report could be used inappropriately, such as a user discussing the information about a victim with others not authorized to know the information.

Mitigation: In order to be granted access to this system, training and education are required on use of information and the Privacy Act initially and annually thereafter. Violators lose the ability to access this database if infractions are identified and reported. Administrative actions are taken once a breach or misuse is verified.

Section 4.0 Notice

4.1 How does the project provide individuals notice prior to the collection of information? If notice is not provided, explain why not.

During the initial meeting with the victim, the SARC explains that the information provided will be placed in DSAID in order to monitor the case from start to conclusion. The victim is also advised that access to this information is limited to individuals with an authorized need to know. Additionally, the victim is given an election form to indicate his or her choice of reporting (i.e., restricted or unrestricted).

USCG provides notice through the SAPR website,[12] on the DoD Helpline, by the Privacy Act Statement on CG-6095 (Victim Reporting Preference Statement), publication of this PIA, and the DHS/USCG-002 Employee Assistance Program SORN.

Additionally, notice posters about the program in general are posted at all USCG units with contact information for SARCs and Victim Advocates.

[12] *See* https://www.dcms.uscg.mil/Our-Organization/Assistant-Commandant-for-Human-Resources-CG-1/Health-Safety-and-Work-Life-CG-11/Office-of-Work-Life-CG-111/Sexual-Assault-Prevention-and-Response-Program/.

4.2 What opportunities are available for individuals to consent to uses, decline to provide information, or opt out of the project?

All individuals that report a sexual assault must sign CG-6095 (Victim Reporting Preference Statement) to participate in SARC services. Victims of sexual assault have two options when reporting information regarding an incident: Unrestricted or Restricted Reporting. Individuals may consent to a full collection of information by making an Unrestricted Report, which will initiate legal proceedings, or they may make a Restricted Report that enables them to receive assistance without legal obligation. A victim that choses to make a restricted report is still authorized to receive advocacy, legal counsel through the Special Victims Counsel, medical treatment, and counseling.

4.3 Privacy Impact Analysis: Related to Notice

Privacy Risk: Individuals may not be fully aware of how their information is used in DSAID.

Mitigation: SARC mitigates this risk by reading and providing notice to the individual at the initial consultation. Additionally, publication of this PIA and the DHS/USCG-002 Employee Assistance Program SORN provide notice.

Privacy Risk: Alleged perpetrators may not know that they have been accused of misconduct and therefore have no notice that their information is collected and maintained in DSAID.

Mitigation: This risk is partially mitigated. Although alleged perpetrators may not know that their information was entered into DSAID, they are investigated by Coast Guard Investigative Service (CGIS) and are made aware that they have been accused of misconduct during that time.

Section 5.0 Data Retention by the project

5.1 Explain how long and for what reason the information is retained.

All DSAID records are cutoff at the end of the fiscal year, in which the sexual assault case is closed and destroyed 50 years after cutoff (AUTH: N1-330-08-07, Item 1).

5.2 Privacy Impact Analysis: Related to Retention

Privacy Risk: Records may be lost, misplaced, or held for longer than required.

Mitigation: Records are 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 and associated PIN. Further, at the DoD-level, only de-identified data for open cases can be accessed. Records are kept in

DSAID for 50 years, after which records are destroyed in a way that precludes recognition or reconstruction in accordance with DoD 5200.1-R, "Information Security Program."[13] Technical guidance is provided by the National Security Agency/Central Security Service (NSA/CSS) System and Network Analysis Center concerning appropriate methods, equipment, and standards for destroying classified electronic media, IT equipment, electronic components, and other similar or associated material.

Section 6.0 Information Sharing

6.1 Is information shared outside of DHS as part of the normal agency operations? If so, identify the organization(s) and how the information is accessed and how it is to be used.

Yes. DSAID is an external DoD centralized case-level sexual assault system for all military services. Data within the DSAID system is shared with DoD Tier 4 system administrators, who have role-based access. The administrators also monitor and provide support to all users of the system. However, PII is not shared among other Departments of the Armed Forces.

6.2 Describe how the external sharing noted in 6.1 is compatible with the SORN noted in 1.2.

DSAID external data sharing is consistent with the routine uses J and M, cited in the DHS/USCG-002 Employee Assistance Program (EAP) Record SORN. These routine uses permit the USCG to share statistical and PII data with the EAP for counseling and treatment purposes, as well as DoD Tier 4 system administrators that serve as the helpdesk for users of the system.

6.3 Does the project place limitations on re-dissemination?

The USCG SARC and DoD Sexual Assault Prevention & Response Office administrators are not allowed to re-disseminate data that is sensitive or contains PII. However, the aggregated, de-identified data is shared, for example to Congress, as part of DoD's reporting requirements. Outside of the system, PII is not shared.

6.4 Describe how the project maintains a record of any disclosures outside of the department.

The system consists of the shared database and personnel authorized access to information for the purpose of facilitating services for victims. Referrals are provided to the victim, but only the victim can disclose his or her PII when seeking desired care outside of the Department. Those working in the area of sexual assault prevention who gather PII are prohibited from releasing this

[13] *See* https://www.hsdl.org/?view&did=506.

information unless a signed authorization is completed by the victim to do so**.**

6.5 Privacy Impact Analysis: Related to Information Sharing

Privacy Risk: There is risk that information could be inadvertently shared with other personnel that do not have a need to know.

Mitigation: The DSAID information collected is only available and accessible to authorized USCG SARCs who have a need to know. Records are maintained in controlled facilities that employ physical restrictions and safeguards such as security guards, identification badges, key cards, and locks. Disclosures authorized by victim by a signed release, is maintained in a double-locked file by the USCG SARC managing the case. Records are kept in DSAID for retrieval and analysis purposes for 50 years, after which records are destroyed in a way that precludes recognition or reconstruction in accordance with DoD 5200.1-R, "Information Security Program."

Section 7.0 Redress

7.1 What are the procedures that allow individuals to access their information?

Individuals seeking access to their data may submit a Freedom of Information Act (FOIA) or Privacy Act request in writing to USCG, Commandant (CG-611), 2703 Martin Luther King Jr Avenue SE STOP 7710, Attn: FOIA Coordinator, Washington, DC 20593-7710. A request may also be submitted to EFOIA@uscg.mil.

7.2 What procedures are in place to allow the subject individual to correct inaccurate or erroneous information?

Individuals may seek to correct their information through a Privacy Act request as cited in Section 7.1 above.

7.3 How does the project notify individuals about the procedures for correcting their information?

Individuals are provided notification of these procedures to correct their information through this PIA and DHS/USCG-002 Employee Assistance Records.

7.4 Privacy Impact Analysis: Related to Redress

Privacy Risk: An individual may not obtain access or have the opportunity to correct or amend their record.

Mitigation: Individuals can obtain access, and correct or amend their record by following the procedures cited above. Individuals may contact individual SARCs associated with their case to answer questions related to redress.

Section 8.0 Auditing and Accountability

8.1 How does the project ensure that the information is used in accordance with stated practices in this PIA?

DSAID data is protected through role-based access and Common Access Card-enabled functionalities. It provides limited access to the system and specific functional areas of the system to ensure data has not been altered or destroyed in an unauthorized manner. Through the use of encryption and firewall protection, PII in transit to or held in DSAID cannot be made available or disclosed to unauthorized individuals, entities, or processes.

Furthermore, audit reviews are conducted to assess the adequacy of maintaining, managing, and controlling events that may degrade the security posture of DSAID's capabilities.

8.2 Describe what privacy training is provided to users either generally or specifically relevant to the project.

DHS privacy training is required for all USCG personnel. Additionally, DoD training is provided for users of DSAID; security training is also provided to educate users to DSAID's security requirements. The system displays reminders to ensure users remain aware of their responsibilities to protect PII.

8.3 What procedures are in place to determine which users may access the information and how does the project determine who has access?

Only trained/nationally credentialed SARCs and legal personnel (involved with the case) will be given access, and each must have a Secret clearance to access the database. Additionally, formal and informal training is provided by DoD.

System access to case files is limited to the victim's SARC, Military Service Sexual Assault Prevention and Response program managers, and authorized Military Service legal officers. DSAID sits on the Office of the Secretary of Defense network. The protections on the network include firewalls, passwords, encryption of data in transit, and web-common security architecture.

8.4 How does the project review and approve information sharing agreements, MOUs, new uses of the information, new access to the system by organizations within DHS and outside?

A memorandum of understanding has been completed between USCG and DoD. The memorandum was vetted through USCG legal and all terms agreed upon prior to USCG use of this system.

DoD Sexual Assault Prevention & Response Office and USCG DSAID program managers are responsible for approving information sharing agreements and memoranda of understanding and granting access to new users of the system. The DoD Sexual Assault Prevention & Response Office hosts a monthly Change Control Board to review any and all changes within this system. This board consists of representatives from all the uniformed services and regular review of the project occurs during these meetings. Any revised sharing agreement will be sent to the USCG Privacy Office (CG-6P) for review.

Responsible Officials

Dr. Marta Denchfield
Chief, Behavioral Health Services Division COMDT (CG-1111)
United States Coast Guard

Approval Signature

Original signed and on file with the DHS Privacy Office.

_____

Jonathan R. Cantor
Acting Chief Privacy Officer
Department of Homeland Security

Appendix: Forms used within DSAID System

CG Form 6095, "Victim Reporting Preference Statement"

DD Form 2911, "DOD Sexual Assault Forensic Examination Report"

DD Form 2965, "Defense Sexual Assault Incident Database (DSAID) Data Form"