OFFICE OF THE SECRETARY OF DEFENSE
SEXUAL ASSAULT PREVENTION AND RESPONSE OFFICE

Defense Sexual Assault Incident Database (DSAID)

Requirements Package Overview and Supplemental Requirements

Version 1.6.3

1401 Wilson Boulevard, Suite 402 ♦ Arlington, Virginia 22209 ♦ 703-696-9422 ♦ www.sapr.mil

Table of Contents

1 Overview

The Defense Sexual Assault Incident Database (DSAID) Requirements Package provides the Developer and Implementer (D&I) with the official requirements that must be included in the design, development, and implementation of DSAID. The DSAID Requirements Package version 1.6.3 (this version) is created from baseline version 1.6.2 and incorporates the changes approved in DSAID Change Memos #27 through #29. The package consists of a variety of documents for DSAID Task Order #2 and #3, including:

- DSAID Requirements Package Overview and Supplemental Requirements (this document).
- DSAID Use Case Models.
- DSAID Use Cases.
- DSAID Report and Ad-Hoc Queries Specification.
- DSAID Standard Service Report Template.
- DSAID (Military Service Academy) MSA Report Template.
- DSAID Data Requirements.
- DSAID and Air Force Systems Interface Data Mapping.

The requirements documents specific to DSAID Task Order #2 include:

- UC 1 – Maintain Victim Case Profile.
- UC 2 – Search DSAID Case.
- UC 3 – View DSAID Case.
- UC 4 – Transfer DSAID Case Between SARCs.
- UC 5 – Upload Air Force Subject and Incident Information.
- UC 6 – Maintain Subject Disposition Information.
- UC 7 – Transfer Incident File Within and Across Service MCIOs.
- UC 8 – Generate SAFE Kit Expiration Notification.
- UC 9 – View SAFE kit Expiration Notification.
- UC 10 – Retrieve Unexpired SAFE Kit Information.
- UC 11 – Convert Restricted Case to Unrestricted Case.
- UC 12 – Close DSAID Case.
- UC 13 – Maintain SARC Profile.
- UC 14 – Maintain SAPR Related Training.
- UC 15 – Maintain Victim Advocate Profile.
- UC 16 – Search Location Code.
- UC 17 – Maintain Memorandums of Understanding (MOU).
- UC 18 – Maintain Case Review Meeting Minutes.
- UC 22 – Generate Standard Reports and Ad-Hoc Queries.
    - Sections related to Ad-Hoc Queries only.
- UC 25 – Register User Account.
- UC 26 – Approve User Account.
- UC 27 – Login.
- DSAID Use Case Models.
    - Case Management.
    - Safe Kit.

    - Business Management.
    - User Account Registration and Login.
- DSAID Report and Ad-Hoc Queries Specification.
    - Ad-Hoc Report Section Only.
- DSAID Data Requirements.
    - All Tabs except for DoD Reporting.
- DSAID and Air Force Systems Interface Data Mapping.

The requirements documents specific to DSAID Task Order #3 include:

- UC 19 – Maintain Combat Zones List.
- UC 20 – Maintain End Strength Data.
- UC 21 – Preschedule Standard Reports.
- UC 22 – Generate Standard Reports and Ad-Hoc Queries.
    - Sections related to Standard Reports only.
- UC 23 – Retrieve Standard Reports.
- DSAID Use Case Models.
    - DoD Reporting.
- DSAID Data Requirements.
    - DoD Reporting Tab.
- DSAID Report and Ad-Hoc Queries Specification.
- DSAID Standard Service Report Template.
- DSAID MSA Report Template.

The documents were compiled based on analysis of the Department of Defense (DoD) Sexual Assault Prevention and Response Data Collection & Reporting System Concept Design Report; multiple Annual Reports on Sexual Assault in the Military and Military Service Academies; extensive information provided by Sexual Assault Prevention and Response Office (SAPRO); interviews from Service stakeholders; and knowledge of similar systems. If the DSAID Requirements Package needs to be changed after the contract is awarded, the request must be approved by a DSAID Change Control Board (CCB) before execution.

2 DSAID Benefits

DSAID will provide the following benefits:

- Multiple levels of trend identification and analysis.
- Standardized reporting to Congress, DoD, and Service leadership.
- Accurate and timely reporting.
- SAPRO and Service Sexual Assault Prevention and Response (SAPR) program management, program planning, and prevention activities support.
- DoD SAPRO Oversight activities support.
- DoD source for internal and external response requests for statistical data on sexual assault.
- Enhanced transparency of sexual assault-related data.
- Enhanced analysis capabilities.
- Semantic interoperability between systems within DoD.

3 Project Approach

DSAID will follow the industry-recognized software development life cycle (SDLC); define, design, develop and test, implement, and maintain. This will result in DSAID functionality being approved during each phase of the SDLC. This iterative process will allow SAPRO and the D&I to be involved throughout the project and will provide a method for addressing, analyzing, and mitigating high-risk items early in the development life cycle of DSAID. All functionality must receive initial approval by SAPRO during the design phase in order to minimize the amount of time and cost for design and code adjustments.

In addition, the requirements and development efforts will be contained within a suite of tools that provide consistency in deliverables and allow for better change control to baseline requirements and/or system development. Specifically, the suite of tools will provide life cycle management and control of software development assets; the ability to track defects and changes; a central console for test activity management, execution, and reporting; electronic management of the requirements; and documentation of the software development process from start to finish.

DSAID will include the development of five major functional capabilities: reporting, data entry, data interface, case management, and business management. These functional capabilities will be designed, developed, tested, and implemented in the phases documented in sections 3.1 through 3.5.

3.1 Define

The requirements outlined in this *DSAID Requirements Package Overview and Supplemental Requirements* document, as well as the *DSAID Use Case Model, the DSAID Use Cases; DSAID Report and Ad-Hoc Queries Specification*; *DSAID Data Requirements*; *DSAID and Air Force Systems Interface Data Mapping; DSAID and Army Systems Interface Data Mapping; DSAID and Navy Systems Interface Data Mapping;* and *DSAID and Marine Corps Systems Interface Data Mapping* represent the SAPRO and Service-approved requirements for DSAID. The DSAID Requirements Package is the basis for DSAID development.

3.2 Design

Due to the overall complexity of DSAID, the design phase will follow a proof-of-concept approach. This approach will allow SAPRO to review each piece of designed functionality within this phase. Each design proof-of-concept must be approved by SAPRO before creation of the next design proof-of-concept can begin. This will enable SAPRO to validate new design ideas early in the process and eliminate issues being found many months into development. Additionally, the use of design proof-of-concepts will allow SAPRO to confirm initial thoughts on DSAID's appearance and functionality, and the D&I to ensure a full understanding of the requirements.

To achieve this, the D&I shall collaborate with SAPRO to complete the following iterative actions:

- Conduct requirements review sessions to ensure the D&I fully understands the approved requirements (SAPRO, D&I).
- Create wireframes/screenshots based on requirements review sessions (D&I).
- Conduct wireframe/screenshot review sessions (SAPRO, D&I).
- Approve final wireframes/screenshots (SAPRO).

The D&I shall use the documented requirements to create a DSAID Design document that will provide a linkage from the requirements to the design of DSAID. The DSAID Design document will include wireframes and/or screenshots when necessary.

3.3 Develop and Test

3.3.1 Develop

After the design proof-of-concepts are approved by SAPRO, the D&I shall begin the creation of development proof-of-concepts. As with the design phase, this process will allow SAPRO and the D&I to be involved throughout this phase, enabling SAPRO the opportunity to review each piece of functionality. Each development proof-of-concept must be approved by SAPRO before creation of the next development proof-of-concept can begin. The D&I shall develop all of the documented requirements.

To achieve this, the D&I shall collaborate with SAPRO to complete the following iterative actions:

- Develop mock-ups within technical solution based on approved wireframes/screenshots (D&I).
- Conduct mock-up review sessions to ensure proper requirements are captured and the design is consistent with intent (SAPRO, D&I).
- Approve developed mock-ups (SAPRO).

The D&I shall update the DSAID Design document once the mock-ups are approved and, when necessary, after development has begun to ensure the proper linkage from the requirements to the developed functionality in DSAID is documented.

3.3.2 Test

The D&I shall set up a development environment using virtual servers on the D&I network that mimic the production server environment at Washington Headquarters Services (WHS) where possible.

The D&I shall perform a series of internal tests as documented in the DSAID Test Plan to ensure all functionality works properly. The D&I shall be responsible for fixing or mitigating the findings based upon the execution results of Security Readiness Review scripts (SRRs), the Defense Information Systems Agency (DISA) Field Security Operations (FSO) Gold Disks, and the Retina Scans on all systems. The D&I must ensure DSAID is in compliance with the security requirements associated with the Defense Information Systems Agency (DISA) Security and Technical Implementation Guides

(STIGS), as specified in section 5.3. Once the internal tests are completed, SAPRO will conduct additional testing as documented in the DSAID Test Plan.

3.4 Implement

Once all of the functionality is approved DSAID will be installed in the WHS production environment and again tested as documented in the DSAID Test Plan.

DSAID will be implemented using a phased approach. The scope and quantity of users that will be included in the implementation will be determined by SAPRO. The D&I shall be responsible for assisting SAPRO to ensure that DSAID is in compliance with all federal and DoD regulations identified in Section 5.1 "Guidance/Reference" of this document.

3.5 Maintain

Following the release of DSAID, SAPRO will continue to gather additional requirements as well as manage the training and the delivery of user manuals. The D&I shall support SAPRO where necessary and provide production environment assistance as required.

4 High-Level Requirements and Guidance

This section defines and documents DSAID high-level requirements and guidance. At a minimum it is envisioned that DSAID will:

- Be a customizable and configurable Commercial-off-the-Shelf (COTS) Case Management System (CMS).
- Be a flexible, user-friendly platform.
- Preserve Service-specific capabilities and systems whenever possible.
- Encompass data security.

In addition, historical data will not be converted into DSAID and it will not contain data related to the following:

- Health Insurance Portability Accountability Act (HIPAA).
- Domestic violence.
- Sexual harassment.

The following sub-sections document high-level guidance that DSAID must be in compliance with, as well as, DSAID high-level supplemental and functional requirements:

4.1 Guidance/Reference

4.1.1 Department of Defense (DoD) Issuances:

DSAID must adhere to all applicable sections of the following Department Issuances:

- DoD Instruction 6495.02, "Sexual Assault Prevention and Response Program Procedures" Incorporating Change 1, November 13, 2008.
- DoD Directive 6495.01, "Sexual Assault Prevention and Response Program" Incorporating Change 1, November 7, 2008.

- DoD Directive 8320.02, "Data Sharing in a Net-Centric Department of Defense".
- DoD Directive 8000.1, Management of the Department of Defense Information Enterprise, February 29, 2009.
- DoD Instruction 4630.8, "Procedures for Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS)" June 30, 2004.
- DoD Directive 4630.5, "Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS)" May 5, 2004.
- Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 6212.01E Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS), December 15, 2008.
- Chairman of the Joint Chiefs of Staff Manual (CJCSM) 6510.01 Information Assurance (IA) and Computer Network Defense (CND).
- DoD Instruction 8551.1, "Ports, Protocols, and Services Management" August 13, 2004.

4.1.2 Federal and DoD Regulations:

DSAID must be in compliance with the following federal and Department of Defense regulations:

- Federal Information Security Management Act of 2002.
- DoD Directive 8500.1, Information Assurance, October 24, 2002.
- DoD Directive 8500.2, Information Assurance (IA) Implementation, February 6, 2003.
- Disposition of Unclassified Computer Hard Drives Memorandum, June 4, 2001.
- Defense Incident Based Reporting System (DIBRS) compatible.
- Section 508 of the Rehabilitation Act of 1973.
- DoD Information Assurance Vulnerability Alert (IAVA) Memorandum, December 30, 1999.
- DoD Directive 8510.01, DoD Information Assurance Certification and Accreditation Process (DIACAP) November 28, 2007 including but, not limited to:
    - Identification of Essential Functions to Prevent Threat (Control Number COEF-1).
    - Trusted Recovery Procedure (Control Number COTR-1).
    - Data Backup Procedures (Control Number CODB-1).
    - Best Security Practices (Control Number DCBP-1).
    - System State Changes (Control Number DCSS-1).
    - Enclave Boundary Defense (Control Number EBBD-2).
    - Resource Control (Control Number ECRC-1).
    - Individual Identification and Authentication (Control Number IAIA-1.

4.1.3 DoD Statutory and Regulatory Requirements:

DSAID must adhere to all applicable DoD statutory and regulatory requirements for system acquisition as listed in the:

- DoD Directive 5000.1 Defense Acquisition Systems, May 12, 2003.
- DoD Issuance 5000.02 "Operation of the Defense Acquisition System" December 2, 2008.
- DoD's defense business systems investment review process, including Human Resources Management (HRM) Investment Review Board (IRB) specific requirements.
- DoD Information Technology Standards Registry (DISR).
- Public Law 104-106: Clinger-Cohen Act of 1996, February 10, 1996.
- Public Law 104-113: National Technology Transfer and Advancement Act of 1995. 104th Congress, March 7, 1996.
- Public Law 93-579: Privacy Act of 1974.

4.2 Functional

4.2.1 Acronyms and Abbreviations

The following acronyms and abbreviations are used in the remaining sections of this document.

FEAT	Feature
INTF	Interface Requirements
SUPP	Supplemental Requirements

4.2.2 FEAT6 Data Elements

FEAT6.1 DSAID must capture and maintain, at a minimum, the data elements documented in the DSAID Data Requirements to include data elements necessary to capture:

FEAT6.1.3 Victim case management data (Restricted and Unrestricted).
FEAT6.1.4 Incident data (Restricted and Unrestricted).
FEAT6.1.5 Subject demographic data (Unrestricted).
FEAT6.1.7 Subject disposition data (per Congressional requirements and as defined by SAPRO/Services) (Unrestricted).
FEAT6.1.8 SAPR program administration data.

4.2.3 FEAT7 Case Management

FEAT7.1 DSAID must allow the creation and maintenance of a DSAID case consisting of information pertinent to victim, incident, subject demographic, and subject disposition in support of tracking a DSAID case from open to close.
FEAT7.2 DSAID must display a DSAID case in a holistic view from either a case search or a user work queue.
FEAT7.3 DSAID must convert a restricted case to an unrestricted case.
FEAT7.4 DSAID must transfer and track individual victim cases between Sexual Assault Response Coordinators (SARCs) and between Services.

FEAT7.5 DSAID must generate a unique DSAID identifier for each victim within DSAID using a combination of business rules.
FEAT7.6 DSAID must be able to search DSAID entities including, but not limited to, a case or a victim.
FEAT7.7 DSAID must generate user notifications within DSAID pertinent to the sexual assault forensic examination (SAFE) kit expiration for a restricted case.
FEAT7.8 DSAID must allow the user to close a DSAID case based upon a set of business rules.
FEAT7.9 DSAID must provide an ability to create, maintain, and display the relationship between the DSAID Case (one victim only), the incident, the subject(s), and any other DSAID case(s) associated with the same incident and subject(s).

4.2.4 FEAT8 Data Query and Reporting

FEAT8.1 DSAID must generate and store a set of Standard Reports based on pre-defined reporting items and user specified criteria.
FEAT8.2 DSAID must allow the user to export and save the Standard Reports to a local drive.
FEAT8.3 DSAID must allow the user to retrieve stored Standard Reports upon the user request within DSAID.
FEAT8.4 DSAID must provide ad-hoc query capabilities using searchable DSAID data elements as the selection criteria.
FEAT8.5 DSAID must allow the user to export and save query results to a local drive.
FEAT8.6 DSAID must maintain the DoD combat zones list.
FEAT8.7 DSAID must maintain end strength data.
FEAT8.8 DSAID must allow the user to pre-schedule Standard Reports and provide a notification to the user once the pre-scheduled Standard Reports are generated.

4.2.5 FEAT9 Data Entry (manual) and Data Interface (electronic)

FEAT9.1 DSAID must collect, track, maintain, manage, and analyze case-level victim, subject demographic, incident, and subject disposition specific information via data entry or Service-specific system interfaces.
FEAT9.2 DSAID must interface with multiple systems with differing technologies and platforms to accommodate the Services that do not or partially use DSAID as a case management system.
FEAT9.3 DSAID must load data via interface to populate the DSAID database periodically.
FEAT9.4 DSAID must associate the source case record with the existing DSAID data (when designated) to properly perform updates/overwrites and avoid redundant data entry.
FEAT9.5 DSAID must accommodate the information variation and Service-specific availability for data load and internal reporting requirements.

FEAT9.6 DSAID must validate the incoming data from source systems to ensure data validity and integration as defined in the DSAID Data Requirements.
FEAT9.7 DSAID must provide the capability to run interfaces "on demand" to request data from Service-specific systems and allow for timely responses to departmental and Congressional inquiries.

4.2.6 FEAT10 Business Management Functionality

FEAT10.1 DSAID must generate lists of cases due for case management group meetings.
FEAT10.2 DSAID must record, generate, and store consolidated meeting minutes and meeting minutes for each DSAID case.
FEAT10.3 DSAID must store Memorandums of Understanding (MOU) records.
FEAT10.4 DSAID must allow certain users to maintain all Victim Advocate profiles.
FEAT10.5 DSAID must allow certain users to maintain all Sexual Assault Response Coordinator (SARC) Profiles.
FEAT10.6 DSAID must maintain training provided by Sexual Assault Response Coordinators (SARCs) and/or other individuals and organizations.

4.3 FEAT5 Technical

FEAT5.4 DSAID must contain business intelligence.
FEAT5.7 DSAID must maintain case-level data.
FEAT5.12 DSAID must encompass proven web-technology standards.
FEAT5.13 DSAID must maintain data integrity.
FEAT5.14 DSAID must execute data synchronization.
FEAT5.15 DSAID must enable data standardization.
FEAT5.16 DSAID must easily export data for analysis in computerized statistical applications, such as Statistical Package for the Social Sciences (SPSS) or Predictive Analytics SoftWare (PASW).
FEAT5.18 DSAID must execute electronic notifications to DSAID users.
FEAT5.20 DSAID must be a centralized repository for Service-specific case-level sexual assault data.
FEAT5.22 DSAID must contain capabilities to extract, transform and load data.
FEAT5.24 DSAID must adhere to the following attributes: performance, scalability, security, availability, usability, supportability, audit history, and configuration.
FEAT5.25 DSAID must control system access based on user roles and permissions.

5 Supplemental Requirements

5.1 SUPP1 Performance

SUPP1.1 DSAID shall generate Standard Reports upon a user's request, not to exceed 10 minutes.
SUPP1.2 DSAID shall return ad-hoc query results within 30 seconds.
SUPP1.3 DSAID shall download all web pages within three seconds during an average load, and five seconds during a peak load.

5.2 SUPP2 Scalability

SUPP2.1 DSAID shall support a minimum of 200 concurrent users and a maximum of 700 concurrent users.
SUPP2.2 DSAID shall support up to 1000 users.
SUPP2.3 DSAID shall maintain consistent performance and response time without noticeable degradation due to increase in the following conditions including, but not limited to:

SUPP2.3.1 Number of users.
SUPP2.3.2 Data type/volume relating to victims, subject demographics, incidents, subject dispositions, and other supporting data elements (subject to regular review; the addition of new data elements, and system capabilities to be a matter of agreement between SAPRO and the reporting Services).
SUPP2.3.3 Number of system interfaces.
SUPP2.3.4 Number of reporting requests submitted by users simultaneously.
SUPP2.3.5 Number of ad-hoc query requests submitted by users simultaneously.

5.3 SUPP3 Security

SUPP3.1 DSAID shall be Common Access Card (CAC)-enabled.
SUPP3.2 DSAID shall employ encryption capability for user access control.
SUPP3.3 DSAID shall allow designated administrators to assign and change user passwords.
SUPP3.5 DSAID passwords shall conform to DoD password standards.
SUPP3.6 DSAID shall log a user off automatically after five minutes of inactivity.
SUPP3.7 DSAID shall capture log-on/off information.
SUPP3.8 DSAID shall display messages for Freedom of Information Act (FOIA) and Personally Identifiable Information (PII).
SUPP3.9 DSAID shall be in compliance with the Privacy Act of 1974 in the Federal Acquisition Regulation (FAR) Clauses 52.224-1 and 52.224-2.
SUPP3.10 DSAID shall display to the user a Government warning message upon logon.

SUPP3.11 DSAID shall support National Institute of Standards and Technology (NIST) encryption standards.
SUPP3.12 DSAID shall implement user account lockout policies for logon attempts.
SUPP3.13 DSAID shall capture at a minimum but not limited to the following information to create a DSAID user account:
User Account Status, User Last Name, User First Name, User Affiliation (Army, Navy, Air Force, Marine Corps, National Guard, and DoD Sexual Assault Prevention and Response Office (SAPRO)), and User Phone Number.
SUPP3.15 DSAID data backup shall be performed at least weekly.
SUPP3.16 DSAID shall be evaluated and validated by either the National Information Assurance Partnership (NIAP) or the Federal Information Processing Standards (FIPS).
SUPP3.17 DSAID shall be in compliance with the Defense Information Systems Agency (DISA) Security and Technical Implementation Guides (STIGS), as applicable to DSAID.

5.4 SUPP4 Availability

SUPP4.1 DSAID shall be available for access and use twenty-four hours a day, seven days a week, with the exception of scheduled maintenance periods.
SUPP4.2 DSAID shall provide access to real-time data.
SUPP4.3 DSAID shall provide access to a case that has been closed for up to five years, for the purpose of Congressional reporting and inquiries.
SUPP4.4 DSAID shall store indefinitely finalized historical Standard Reports.
SUPP4.5 DSAID shall provide real-time access to archived data in electronic format for up to 60 years, excluding film and tape.
SUPP4.6 DSAID shall archive a case after two years of inactivity.

5.5 SUPP5 Usability

SUPP5.1 DSAID shall allow on-screen actions to be performed by both keyboard and mouse.
SUPP5.2 DSAID shall employ standard keystroke shortcuts.
SUPP5.3 DSAID shall be web-based and have a Graphical User Interface (GUI).

5.6 SUPP6 Supportability

SUPP6.1 DSAID shall be a customized and configurable Commercial Off-The-Shelf (COTS) product.
SUPP6.2 DSAID shall adjust to changes to internal or external reporting requirements.
SUPP6.3 DSAID shall adjust to changes to case management functionality.
SUPP6.4 DSAID shall have the capability to export data that is stored in DSAID.
SUPP6.5 DSAID shall be a data warehouse for the storage and collation of data received via interface from Service-systems, data directly entered by authorized system users, and system generated data.

SUPP6.6 DSAID shall be Defense Incident Based Reporting System (DIBRS) compatible.
SUPP6.7 DSAID shall be in compliance with Section 508 of the Rehabilitation Act of 1973.

5.7 SUPP7 Audit History

SUPP7.1 DSAID shall maintain a complete audit history of actions performed in DSAID.
SUPP7.2 DSAID shall capture the following information for each audit record:

- User ID.
- Successful and unsuccessful attempts to access security files.
- Date and time of the event.
- Type of event.
- Success or failure of event.
- Successful and unsuccessful logons.
- Denial of access resulting from excessive number of logon attempts.
- Blocking or blacklisting a user ID, terminal or access port and the reason for the action.
- Activities that might modify, bypass, or negate safeguards controlled by the system.

SUPP7.3 DSAID shall have the capability to review audit records and generate reports from audit records.
SUPP7.4 DSAID shall maintain audit records for at least one year.
SUPP7.5 DSAID shall implement strong access controls to protect against unauthorized access, modification or deletion of audit records.

5.8 SUPP8 User Roles and Permissions

SUPP8.1 DSAID shall allow the user to access a DSAID case based on the permission(s) associated with the assigned user role(s).
SUPP8.2 DSAID shall set up the user role and permission(s) based upon the business rules associated with the use cases.
SUPP8.7 DSAID shall allow a user to have more than one user role assigned to that user's log-on account, if applicable.

5.9 SUPP11 Configuration

SUPP11.3 Pre-Load

SUPP11.3.2 The list of DSAID Location Codes containing military and non-military entries, maintained by SAPRO, shall be pre-loaded.
SUPP11.3.3 The list of countries, maintained by the U.S. Department of State, shall be pre-loaded.
SUPP11.3.4 The list of City and State/Country containing US and International cities, shall be pre-loaded.

6 Interface Requirements

6.1 INTF1 DSAID Air Force I2MS Interface

INTF1.1 DSAID shall provide interface capability to load case-level data from the Air Force's Investigative Information Management System (I2MS).
INTF1.2 DSAID shall load the case-level data provided by I2MS for the sexual assault victim cases as specified by the DSAID and Air Force Systems Interface Data Mapping.

6.2 INTF2 DSAID Army SADMS Interface

INTF2.1 DSAID shall provide interface capability to load case-level data from the Army's Sexual Assault Data Management System (SADMS).
INTF2.2 DSAID shall load the case-level data provided by the Army's Sexual Assault Data Management System (SADMS) as specified by the DSAID and Army Systems Interface Data Mapping.

6.3 INTF3 DSAID Marine Corps SAIRD and CLEOC Interfaces

INTF3.1 DSAID shall provide interface capability to load restricted case-level data from the Marine Corps' Sexual Assault Incident Reporting Database (SAIRD).
INTF3.2 DSAID shall provide interface capability to load unrestricted case-level data from the Department of the Navy's Consolidated Law Enforcement Operations Center (CLEOC).
INTF3.3 DSAID shall load unrestricted and restricted case-level data provided by the Marine Corps' Sexual Assault Incident Reporting Database (SAIRD) and the Department of the Navy's Consolidated Law Enforcement Operations Center (CLEOC) as specified by the DSAID and Marine Corps Systems Interface Data Mapping.

6.4 INTF4 DSAID Navy SAVI CMS and CLEOC Interfaces

INTF4.1 DSAID shall provide interface capability to load restricted case-level data from the Navy's Sexual Assault Victim Intervention Case Management System (SAVI CMS).
INTF4.2 DSAID shall provide interface capability to load unrestricted case-level data from the Navy's Sexual Assault Victim Intervention Case Management System (SAVI CMS) and the Department of the Navy's Consolidated Law Enforcement Operations Center (CLEOC).
INTF4.3 DSAID shall load unrestricted and restricted case-level data provided by the Navy's Sexual Assault Victim Intervention Case Management System (SAVI CMS) and the Department of the Navy's Consolidated Law Enforcement Operations Center (CLEOC) as specified by the DSAID and Navy Systems Interface Data Mapping.