United States Government Accountability Office

Report to Congressional Committees

January 2017

MILITARY PERSONNEL

DOD Has Processes for Operating and Managing Its Sexual Assault Incident Database

GAO Highlights

Highlights of GAO-17-99, a report to congressional committees

January 2017

MILITARY PERSONNEL

DOD Has Processes for Operating and Managing Its Sexual Assault Incident Database

Why GAO Did This Study

GAO has reported that DOD has not collected uniform data on sexual assaults involving members of the armed forces. In 2008, Congress required DOD to implement a centralized, case-level database for the collection and maintenance of these data. In 2012, DSAID reached initial operational capability to capture sexual assault data. House Report 112-479 included a provision for GAO to review DSAID no sooner than 1 year after it was certified compliant with DOD standards by the Secretary of Defense.

This report (1) describes the current status of DOD's implementation of DSAID and steps DOD has taken to help standardize DSAID's use, (2) assesses any technical challenges DSAID's users have identified and any DOD plans to address those challenges, and (3) assesses the extent to which DOD's change management process for modifying DSAID aligns with information technology and project management industry standards.

GAO reviewed DOD documents, and interviewed DOD program officials as well as DSAID users. Specifically, GAO conducted site visits to 9 military installations and met with 42 DSAID users. Views obtained are nongeneralizable. Installations were selected based on their use of DSAID, number of users, geographic diversity, and other factors.

GAO is not making recommendations in this report. DOD provided technical comments, which GAO incorporated as appropriate.

View GAO-17-99. For more information, contact Brenda S. Farrell at (202) 512-3604 or farrellb@gao.gov.

What GAO Found

As of October 2013, the Department of Defense's (DOD) Defense Sexual Assault Incident Database (DSAID) was fully implemented and in use across the military services, and DOD had taken several steps to standardize DSAID's use throughout the department. Sexual assault incident data are input into DSAID through both manual and automated data entry processes and include, as applicable, victim and referral support information, investigative and incident information, and case outcome data for certain incidents of sexual assault that involve a servicemember. Additionally, in some instances DSAID includes sexual assault cases involving a servicemember spouse, an adult family member, and DOD civilians and contractors. Further, DOD has taken several steps to standardize DSAID's use through the development of (1) policies, processes, and procedures for using the system; (2) training for system users; and (3) processes for monitoring the completeness of data.

DSAID users have identified technical challenges with the system and DOD officials stated that they have plans to spend approximately $8.5 million to implement modifications to DSAID that address most of these challenges in fiscal years 2017 and 2018. Some of the key technical challenges users have identified experiencing with the system relate to DSAID's system speed and ease of use; interfaces with other external DOD databases; and users' ability to query data and generate reports. DOD has plans in place to implement modifications to DSAID that are expected to alleviate these challenges; however, officials stated that they will not be approved to fund these modifications until they have conducted an analysis of alternatives that is in line with DOD's acquisition policy framework. This framework, as well as the *GAO Cost Estimating and Assessment Guide*, outline key elements of this analysis, such as relative lifecycle costs and benefits and the effect and value of cost and schedule, among others. Conducting an analysis of alternatives including these elements is key to ensuring that DOD appropriately manages its modifications to DSAID. In 2010, GAO found that DOD had failed to demonstrate adherence to these key elements in the initial development and implementation of DSAID, and, DOD projects it will have spent a total of approximately $31.5 million on implementing and maintaining DSAID through fiscal year 2018. This is approximately $13 million more than the 2012 estimate. DOD's plan to conduct an analysis of alternatives that adequately considers key elements should position DOD to more accurately assess whether planned modifications to DSAID can be implemented within budget and result in the desired outcome.

DOD manages modifications to DSAID through its change management process, which GAO found substantially aligns with key applicable elements established in the industry standards that GAO reviewed. Specifically, DOD has established processes for managing change requests, such as developing a process to evaluate requested changes to the database and establishing a board that approves, tracks, and controls changes to the database. DOD has also established processes for configuration management, including a process to track, communicate, and deliver changes to the database.

Contents

Tables

Figure

Abbreviations

DOD	Department of Defense
DSAID	Defense Sexual Assault Incident Database
IEEE	Institute for Electrical and Electronics Engineers
MCIO	Military Criminal Investigative Organization
PMBOK ® Guide	Guide to the Project Management Body of Knowledge
SAPR	Military Service Sexual Assault Prevention and Response Office
SAPRO	DOD Sexual Assault Prevention and Response Office
SARC	Sexual Assault Response Coordinator

GAO U.S. GOVERNMENT ACCOUNTABILITY OFFICE
441 G St. N.W.
Washington, DC 20548

January 10, 2017

Chairman
Ranking Member
Committee on Armed Services
United States Senate

Chairman
Ranking Member
Committee on Armed Services
House of Representatives

Sexual assault undermines the Department of Defense's (DOD) core values, mission, and combat readiness. In 2008 we reported that historically, DOD has not collected uniform data on the incidence of sexual assaults involving members of the armed forces.[1] We concluded that without consistent, accurate, and reliable department-wide data on incidences of sexual assault in the military, DOD was limited in its ability to identify trends in sexual assault and develop targeted prevention and response efforts. Also, in 2008, Congress required the Secretary of Defense to implement a centralized, case-level database for the collection and maintenance of information regarding sexual assaults involving a member of the armed forces, including information, if available, about the nature of the assault, the victim, the offender, and the outcome of any legal proceedings in connection with the assault.[2]

In 2008, the House Armed Services Committee noted that it intended for DOD to use the database to improve the quality and utility of the analysis and recommendations included in DOD's annual reports to Congress on sexual assault.[3] In response to statutory requirements, the Under Secretary of Defense for Personnel and Readiness assigned responsibility for developing the Defense Sexual Assault Incident

[1] GAO, *Military Personnel: DOD's and the Coast Guard's Sexual Assault Prevention and Response Programs Face Implementation and Oversight Challenges*, GAO-08-924 (Washington, D.C.: Aug. 29, 2008). We conducted this review in response to a provision in Senate Report 110-77. S. Rep. No. 110-77, at 345 (2007).

[2] Duncan Hunter National Defense Authorization Act for Fiscal Year 2009, Pub. L. No. 110-417, § 563 (2008).

[3] H.R. Rep. No. 110-652, at 368 (2008).

Database (DSAID) to DOD's Sexual Assault Prevention and Response Office (SAPRO), and required that the military services use DSAID to collect sexual assault data.[4] In 2012, DSAID became operational and the military services[5] started to use it to capture incident, investigation, and subject disposition data for certain incidents of sexual assault that involved a service-member. [6]

In 2010, we made six recommendations aimed at ensuring that DOD followed key practices for the acquisition and implementation of information technology systems—such as developing an economic justification and system requirements—were followed when developing DSAID.[7] DOD concurred with these recommendations, but did not fully implement them prior to the implementation of DSAID. Our assessment of DOD's efforts to address these recommendations is discussed further in the background section of this report.

House Report 112-479, accompanying a bill for the National Defense Authorization Act for Fiscal Year 2013, included a provision for us to conduct a review of DSAID once the database had been certified by the Secretary of Defense.[8] This report (1) describes the current status of

[4] Department of Defense Directive 6495.01, *Sexual Assault Prevention and Response (SAPR) Program* (Jan. 23, 2012) (incorporating change 2, effective Jan. 20, 2015). SAPRO, which is located in DOD's Office of the Undersecretary for Personnel and Readiness, is responsible for policy related to DOD's sexual assault prevention programs. Each of the military services has a Sexual Assault Prevention and Response (SAPR) program that is responsible for the implementation of DOD's policies. The Army's program, Sexual Harassment/Assault Response and Prevention (SHARP), combines sexual harassment and sexual assault prevention programs.

[5] DSAID is also used by the reserve component and the U.S. Coast Guard. However, this report focuses on DSAID's use by the active component of the Army, the Navy, the Marine Corps, and the Air Force, which we refer to collectively as the military services.

[6] DSAID does not include sexual assault data on intimate partners or children. This information is under the purview of the Family Advocacy Program. Additionally, in some cases DSAID includes data on sexual assault cases involving servicemembers' spouses and adult family members, as well as DOD civilians and contractors.

[7] GAO, *Military Personnel: Additional Actions Are Needed to Strengthen DOD's and the Coast Guard's Sexual Assault Prevention and Response Programs,* GAO-10-215 (Washington, D.C.: Feb. 3, 2010).

[8] According to DOD officials, certification is granted after the program satisfies DOD's Information Assurance Certification and Accreditation (DIACAP) process, which requires compliance with approximately 100 controls. DOD officials said that DSAID met these requirements for certification and was granted authority to operate in March 2012. To ensure DSAID was being used by all of the military services and contained multiple years of data, we began our review in November 2015.

DOD's implementation of DSAID and steps DOD has taken to help standardize DSAID's use, (2) assesses any technical challenges DSAID's users have identified with DSAID and any DOD plans to address those challenges, and (3) assesses the extent to which DOD's change management process for modifying DSAID aligns with information technology and project management industry standards.

For our first objective, we reviewed DOD policies, processes, and procedures pertaining to DSAID operations, and interviewed DOD program officials on actions that have been taken to implement DSAID. Specifically, we reviewed processes to train DSAID users and monitor DSAID data quality. We limited our review to the processes DOD and the services have to monitor data quality, and did not assess the accuracy and completeness of the data contained in DSAID because, at the time of our review, DSAID contained data for fiscal years 2014 and 2015 that had undergone extensive review by DOD to ensure they were accurate and complete prior to their inclusion in DOD's annual reports to Congress. Lastly, we reviewed DOD's DSAID quality assurance tool—the primary tool used to identify errors and omissions in DSAID data—and its methodology for identifying significant errors in DSAID data.

For our second objective, we reviewed DOD documents, which included all DSAID help desk tickets generated between January 2015 and April 2016 (which was approximately 600 tickets). We selected this time period because we found that help desk tickets prior to January 2015 were generally related to the user's inexperience with the system, whereas tickets after that date largely related to technical issues with the system and thus were more germane to our review. We also reviewed all change requests that were submitted between August 2013 and May 2016 by DOD and service officials to the DSAID Change Control Board but had not been implemented (which was approximately 40 change requests). We chose this time period because of our interest in system changes that had been requested and still under consideration, and all change requests submitted prior to August 2013 had already been closed. We also interviewed DOD officials as well as DSAID users and program managers for the Army, the Navy, the Marine Corps, and the Air Force at both service headquarters[9] and at selected installations.[10] Installations were selected to represent a range of user experience with DSAID including (1) number of cases in DSAID, (2) number of Sexual Assault Response Coordinators (SARC), (3) number of DSAID data errors identified by SAPRO's quality assurance tool, and (4) geographic diversity. Specifically, we selected 9 installations—Joint Base Langley-Eustis, Virginia; Naval Station Norfolk, Virginia; Goodfellow Air Force Base, Texas; Fort Hood, Texas; Naval Base San Diego, California; Naval Base Coronado, California; Marine Corps Air Station Miramar, California; Marine Corps Base Quantico, Virginia; and Fort George G. Meade, Maryland. At these locations, SARCs representing the following 4 additional installations were in attendance as well—Marine Corps Base Camp Pendleton, California; Marine Corps Recruit Depot San Diego, California; Presidio of Monterey, California; and Naval Base Point Loma, California.

During site visits, we met with 42 SARCs representing 13 installations in the United States. Views we obtained from these SARCs were not generalizable. We evaluated the information we obtained from these documents and interviews to identify any technical challenges users faced in operating DSAID, as well as any systemic challenges DOD had identified with DSAID. We interviewed DOD officials to determine whether they had plans to address any challenges identified, and how costs for these plans were determined. To assess the process DOD used for estimating costs to modify DSAID, we compared the process DOD used to estimate the costs of any planned modifications with best practices for cost estimating and assessment in the GAO Cost Estimating and Assessment Guide.[11] We reviewed DOD documents and interviewed DOD officials to obtain information on its costs incurred since the initial DSAID contract was granted in August 2010 through October 2016.

[9] We met with officials from the Air Force, the Navy, and the Marine Corps Sexual Assault Prevention and Response Offices as well as with officials from the Army's Sexual Harassment/Assault Response and Prevention Office. For the purposes of this report, we refer to these officials and programs as SAPR.

[10] For the purposes of our report, we did not include the reserve component and the U.S. Coast Guard in our scope.

[11] GAO, *GAO Cost Estimating and Assessment Guide: Best Practices for Developing and Managing Capital Program Costs (Supersedes* GAO-07-1134SP*),* GAO-09-3SP (Washington, D.C.: Mar. 2, 2009). This guide focuses on developing cost estimates for government capital acquisition programs, but it outlines best practices that are applicable to cost estimation in general.

For our third objective, we reviewed elements of DOD's change management and configuration management processes that were applicable to our scope. Specifically, we focused on elements that are managed by DOD, such as processes for, managing change requests and configuration control activities for configuration status accounting, interface control, and release management. We compared these elements with the Project Management Institute's A Guide to the Project Management Body of Knowledge (PMBOK® Guide), Fifth Edition, 2013 and the Institute of Electrical and Electronics Engineers' (IEEE) Standard for Configuration Management in Systems and Software Engineering to determine how DOD's process for managing changes to DSAID aligned with project management and information management industry standards applicable for implementing and monitoring change and configuration management in established information technology systems.[12] We selected the Project Management Institute's criteria because it provides guidelines that are relevant to project managers and project teams on the requirements and responsibilities of sound change management and configuration management systems for their project. We have used the PMBOK® Guide in multiple reports that address a variety of topics for which project management standards are applicable.[13] We selected IEEE's criteria because it establishes minimum process requirements for configuration management in systems and software engineering and because it can be applied to any form, class, or type of software or system. We have used IEEE standards as guidance

[12] Project Management Institute, Inc*., A Guide to the Project Management Body of Knowledge (PMBOK® Guide) –Fifth Edition* (Newtown Square, Pa.: 2013). PMBOK is a trademark of Project Management Institute, Inc. The PMBOK® Guide is the accepted standard describing the project management process and the management of individual projects throughout their life cycles. Institute of Electrical and Electronics Engineers', *IEEE Standard for Configuration Management in Systems and Software Engineering*. *IEEE Std 828TM-2012* (Revision of IEEE Std 828-2005), March 16, 2012. Organizations use configuration or change management processes to control changes to the characteristics of an existing system. Change management processes include recording and reporting each change and its implementation status as well as supporting the audit of products to verify conformance to requirements. Through these change management mechanisms, an organization can establish and protect the integrity of a product throughout its lifecycle.

[13] See, for example, GAO, *Defense Major Automated Information Systems: Cost and Schedule Commitments Need to Be Established Earlier,* GAO-15-282 *(*Washington, D.C.: Feb. 26, 2015) and GAO, *Information Technology: FEMA Needs to Address Management Weaknesses to Improve Its Systems,* GAO-16-306 (Washington, D.C.: Apr. 5, 2016).

for information technology best practices in previous reports that address a variety of topics.[14]

We conducted this performance audit from November 2015 to January 2017 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Background

In October 2004, Congress included a provision in the Ronald W. Reagan National Defense Authorization Act for Fiscal Year 2005 that required the Secretary of Defense to develop a comprehensive policy for DOD on the prevention of and response to sexual assaults involving members of the armed forces.[15] In part, the legislation required DOD to develop a uniform definition of "sexual assault" for all the armed forces and submit an annual report to Congress on reported sexual assault incidents involving members of the armed forces. The statute also required the Secretaries of the military departments to prescribe procedures for confidentially reporting sexual assault incidents.

DOD issued its first annual report to Congress in May 2005, and in August 2008 we conducted a review that, among other things, evaluated the extent to which DOD had visibility and exercised oversight over reports of sexual assault involving servicemembers.[16] We found that DOD's annual reports to Congress may not effectively characterize incidents of sexual assault in the military services because the department had not clearly articulated a consistent methodology for reporting incidents and because the means of presentation for some of the data did not facilitate their comparison. Further, we found that while DOD's annual reports to Congress included data on the total number of

[14] See, for example, GAO, *HEALTHCARE.GOV CMS Has Taken Steps to Address Problems, but Needs to Further Implement Systems Development Best Practices,* GAO-15-238 *(*Washington, D.C.: Mar. 4, 2015) and GAO, *Information Technology: FEMA Needs to Address Management Weaknesses to Improve Its System*, GAO-16-306 (Washington, D.C.: Apr. 5, 2016)

[15] Pub. L. No. 108-375, § 577 (2004).

[16] GAO-08-924

restricted and unrestricted reported incidents of sexual assault,[17] meaningful comparisons of the data could not be made because the offices providing the data to DOD measured incidents of sexual assault differently. As a result, we recommended that DOD improve the usefulness of its annual report as an oversight tool by establishing baseline data to permit analysis of data over time. DOD concurred with this recommendation and has taken steps to develop baseline data through the development of DSAID.

Also, in 2008, Congress mandated that DOD implement a centralized, case-level database for the collection and maintenance of information regarding sexual assault involving a member of the armed forces.[18] Additional mandates have since required the DOD-wide collection of additional data, such as case disposition and military protective orders for annual reporting purposes.[19] We conducted a review of DOD's efforts to implement a centralized sexual assault database, and in 2010 we reported that while DOD had taken steps to begin acquiring a centralized sexual assault database it did not meet the statutory requirement to establish the database by January 2010.[20] Moreover, we found that DOD's acquisition and implementation of DSAID did not fully incorporate key information technology practices related to the following: economic justification, requirements development and management, risk management, and test management. DOD concurred with all of our

[17] DOD's restricted reporting option allows sexual assault victims to confidentially disclose an alleged sexual assault to sexual assault response coordinators, uniformed or civilian victim advocates, and health care personnel. Restricted reporting allows victims to receive medical treatment and counseling services without initiating an official investigation. In contrast, DOD's unrestricted reporting option allows sexual assault victims to receive medical treatment and counseling services and request an official investigation of the allegation using existing reporting channels, such as their chain of command or law enforcement. In addition to including data on victims of sexual assault serving in the armed forces, DSAID may also include data on a servicemember's spouse or adult family member who is sexually assaulted, as well as DOD civilians or contractors who are sexually assaulted.

[18] Pub. L. No. 110-417, § 563(a) (2008).

[19] National Defense Authorization Act for Fiscal Year 2010, Pub. L. No. 111-84, § 567(c) (2009) (requiring DOD to collect information on military protective orders involving sexual assault); Ike Skelton National Defense Authorization Act for Fiscal Year 2011, Pub. L. No. 111-383, § 1631 (2011) (listing additional data to be collected by each of the military services); National Defense Authorization Act for Fiscal Year 2013, Pub. L. 112-239, § 572(b)(2) (2012) (requiring that DOD record the data from section 1631 of public law 111-383 to be incorporated into DSAID).

[20] GAO-10-215.

findings and recommendations and has taken some actions to address them.

- Economic justification: We found that DOD's cost estimate for DSAID ($12.6 million) did not include all costs over the system's life cycle and had not been adjusted to account for program risks. In 2012, DOD reassessed DSAID's costs to include additional expenses not included in the original estimate; however, as of November 2016, DOD has not been able to provide DSAID life cycle documentation that would demonstrate that DOD had taken steps to ensure that all costs and program risks were accounted for.
- Requirements development and management: We found that DOD had taken initial steps to engage some users in the development of DSAID requirements and in 2009 had developed its initial requirements management plan. DOD's initial requirements management plan established processes and guidelines for requirements management activities. This plan has been updated three times with the latest update in January 2016. DOD has some systematic methods in place for tracking user feedback, which is a key step in identifying system requirements. In addition, DOD has elicited feedback on users' experience with DSAID since the database's implementation. For example, in 2012, 2013, and 2015 DOD collected non generalizable feedback from DSAID users, including SARCs, SAPR program managers, and the military services legal officers.
- Risk management: We found that during development of the system, DOD had begun to identify key risks such as staffing shortages and competing priorities among the military services. In 2011, DOD developed a risk management plan that identified risks associated with DSAID. In the risk management plan, DOD assigned probability and impact ratings to some of the identified risks. In addition, DOD reported discussing program risks and technical risks to the database at its management meetings and has an issues tracker to track, among other things, risks to the database. However, as of August 2016, DOD had not demonstrated that it had established and implemented defined processes for mitigating risks identified in its risk management plan.
- Test management: At the time of our review in 2010, DOD officials told us that they were planning, but had not started to work with a development contractor to establish an effective test management structure, develop test plans, and capture and resolve problems found

during testing.[21] As of October 2016, DOD had developed several test management plans.

DOD Has Implemented DSAID across the Military Services and Taken Steps to Standardize Its Use and Monitor Data Quality

DOD Has Implemented DSAID across the Military Services

As of October 2013, DOD had implemented DSAID across the military services, and the military services were using it to track and collect data on sexual assault cases.[22] DSAID has since been used to generate data included in DOD's Annual Reports on Sexual Assault in the Military for Fiscal Years 2014 and 2015, DOD's Fiscal Year 2014 Report to the President of the United States on Sexual Assault Prevention and Response, and DOD's Annual Report on Sexual Harassment and Violence at the Military Service Academies for Academic Program Year 2014-15.

DSAID captures DOD-wide data on reports of sexual assault that allow victims to receive treatment and services. Reports can be "restricted" (i.e., confidential reporting of alleged sexual assault without initiating an investigation) or "unrestricted" (i.e., nonconfidential reporting that may initiate an investigation). Reports of sexual assault included are those in which either the victim of the assault or the subject of the investigation are members of the armed forces, or in some cases, when a victim is a servicemember's spouse or adult family member, or is a DOD civilian or

[21] In 2016, during the course of our review, DOD provided us with user acceptance testing documentation initially developed in December 2011, and updated in December 2015, to capture enhancements added to DSAID and changes made to the testing process.

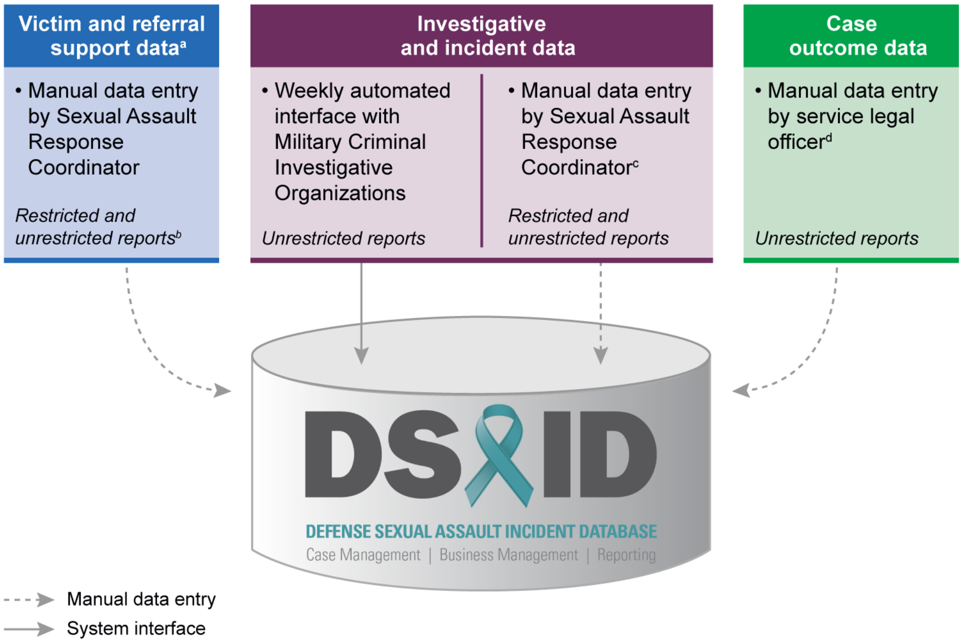
[22] In 2012, DSAID became available to the military services. According to officials from the military services' headquarters-level SAPR offices, the Air Force, the Navy, and the Marine Corps implemented DSAID in 2012 and the Army implemented DSAID in October 2013. The database is also used by the reserve components and the U.S. Coast Guard.

contractor. Data are input into DSAID through both manual and automated data entry processes, and include, as applicable, victim and referral support information; investigative and incident information; and case outcome data. DSAID cases are originated by SARCs, based on a report of sexual assault made by a victim to a SARC, a military service Sexual Assault Prevention and Response (SAPR) victim advocate, or military criminal investigative organization (MCIO) investigator.[23] Generally, victim data are manually input into DSAID by SARCs and investigative data are collected by each military service's MCIO and transferred into DSAID through an automated interface process.[24] For details on DOD's process for inputting data elements into DSAID, see figure 1.

[23] SARCs are the single point of contact for coordinating appropriate and responsive care for a victim when a sexual assault incident is reported. A SAPR victim advocate provides non-clinical crisis intervention, referral, and ongoing nonclinical support to adult sexual assault victims. Support includes providing information on available options and resources to victims. The SAPR victim advocate, on behalf of the sexual assault victim, provides liaison assistance with other organizations and agencies on victim care matters and reports directly to the SARC when performing victim advocacy duties.

[24] MCIOs include the U.S. Army Criminal Investigation Command, the Naval Criminal Investigative Service (which also includes the Marine Corps), and the Air Force Office of Special Investigations.

Figure 1: Department of Defense Process for Inputting Data into the Defense Sexual Assault Incident Database (DSAID)


Victim and referral support data[a]
• Manual data entry by Sexual Assault Response Coordinator
Restricted and unrestricted reports[b]
Investigative and incident data
• Weekly automated interface with Military Criminal Investigative Organizations
Unrestricted reports
• Manual data entry by Sexual Assault Response Coordinator[c]
Restricted and unrestricted reports
Case outcome data
• Manual data entry by service legal officer[d]
Unrestricted reports
DSAID
DEFENSE SEXUAL ASSAULT INCIDENT DATABASE
Case Management | Business Management | Reporting
Manual data entry
System interface

Source: GAO presentation of Department of Defense information. | GAO-17-99

[a] Victim and referral support data include information related to victims' demographics or to the support (e.g., mental health, medical, or spiritual support) offered to victims involved in a sexual assault.

[b] "Restricted" reporting allows victims to confidentially disclose to specified individuals information about a sexual assault without triggering the notification of law enforcement or victims' chain of command, unless a victim consents or an exception applies. "Unrestricted" reporting allows eligible victims to request an official investigation.

[c] Sexual Assault Response Coordinators manually input investigative and incident data into DSAID if the agency conducting the investigation is not a military criminal investigative organization (e.g., civilian law enforcement agency).

[d] Military service legal officers are responsible for entering and approving input into DSAID about the final case disposition.

DSAID can be accessed only by authorized users, who are assigned different access rights depending on their roles and responsibilities pertaining to the collection of sexual assault data. SARCs with DSAID access are required to have a valid DOD Sexual Assault Advocate Certification, and all DSAID users must meet background check and Privacy Act/Personally Identifiable Information training requirements as well as complete user-role specific system training. According to DOD officials, as of July 19, 2016, DSAID had 1,009 users, including 938 SARCs; 34 program managers; 11 SAPRO analysts; 25 military service legal officers; and 1 SAPRO super user See table 1 for a description of the roles and access rights for each of these user groups.

Table 1: Roles and Access Rights for Users of the Defense Sexual Assault Incident Database (DSAID)

User group	Role	Access right to search/view cases	Access right to run ad-hoc queries/reports
SARC	• Collect and input victim and incident data through restricted and unrestricted reports. • Track support to victims throughout the lifecycle of a DSAID case. • Track cases for review.	Yes. Within specific service or assigned location.	No.
Major command or supervisory SARC	• Collect and input victim and incident data through restricted and unrestricted reports. • Track support to victims throughout the lifecycle of a DSAID case. • Track cases for review.	Yes. Within specific service.	No.
Military service SAPR program managers	• Track cases for review. • Produce ad-hoc queries. • Facilitate trend analysis. • Support program planning analysis and management.	Yes. Within service only.	Yes. Role-based permissions.
SAPRO analysts	• Develop data matrixes used in congressionally mandated reports electronically. • Produce ad-hoc queries. • Facilitate trend analysis. • Support program planning analysis and management.	Yes.	Yes. Role-based permissions.
Military service legal officers	• Input case synopsis after investigation is closed and disposition is reached.	Yes. Limited case data within service only.	Yes. Role-based permissions.
SAPRO super user	• Approve and manage SAPRO analyst, military service SAPR program manager, and military service legal officer accounts in DSAID. • Switch between a super user and a SAPRO analyst, which might occur if the super user needs to perform custom queries or access specific data in response to congressional inquiries.	Yes.	Yes. Role-based permissions.

Legend: Sexual Assault Response Coordinator (SARC), Military Service Sexual Assault Prevention and Response Office (SAPR), and DOD Sexual Assault Prevention and Response Office (SAPRO).

Source: GAO analysis of Department of Defense documents. | GAO-17-99

DOD Has Taken Steps to Standardize the Use of DSAID across the Military Services

Since 2012, DOD has taken several steps to standardize the use of DSAID throughout the department, including the development of (1) policies, processes, and procedures for use of the system; (2) training for system users; and (3) processes for monitoring the completeness of data.

Development of Policies, Processes, and Procedures

Since its implementation, DOD has developed multiple policies, processes, and procedures to guide the use of DSAID. Specifically, DOD's sexual assault prevention and response instruction requires that information about sexual assaults reported to DOD involving persons covered by the instruction be entered into DSAID, and also established rules for DSAID access and procedures for entering data.[25] Similarly, three of the services have added and officials from one of the services told us that they are in the process of adding language to their military service- specific sexual assault guidance requiring the use of DSAID. To assist users, DOD also developed a DSAID user manual that is revised with each new system update. Further, DOD's instruction on the investigation of adult sexual assault requires MCIOs to ensure that data obtained through unrestricted reports of sexual assault, such as the investigative case number, are available for incorporation into DSAID.[26] According to DOD officials, this instruction is currently being reviewed to provide more specific instructions to investigators.

Further, DOD has instituted formal processes to facilitate changes to DSAID. In 2011—prior to DSAID becoming fully operational—DOD established its DSAID Change Control Board, which provides a framework to formally manage updates or modifications to the system, and includes representation from each of the military services. The board has a formal charter, is to use established processes and procedures, and members are to meet monthly to discuss proposed changes to the system. In order for a change to be approved, a majority of members must agree to the modification unless there is a legislative or DOD mandate for modification. Through its change control processes, the CCB

[25] Department of Defense Instruction 6495.02, *Sexual Assault Prevention and Response (SAPR) Program Procedures* (Mar. 28, 2013) (incorporating change 2, effective July 7, 2015).

[26] Department of Defense Instruction 5505.18, *Investigation of Adult Sexual Assault in the Department of Defense* (Jan. 25, 2013) (incorporating change 2, June 18, 2015).

approves, prioritizes, and implements change requests.[27] As of October 2016, there have been 135 change requests submitted since the system became operational in 2013—56 of which have been implemented through the change control process.

Development of Training for DSAID Users

DOD has developed and conducted several training courses for DSAID users. Initially, DSAID users were required to attend in person training on DSAID prior to being granted access to the system. However, as of April 2013, DOD converted this required training from in person to a web-based self-guided training that consists of simulations demonstrating DSAID's capabilities. Further, a DOD official told us that SAPRO conducts in-person training for program managers as well as virtual training for military services' legal officers. In addition, since June 2013, DOD has hosted a regular webinar series to inform and train users on a range of DSAID topics, including policy, new releases, or updates to DSAID. According to DOD officials, as of April 2016, DOD had implemented required annual refresher training for program managers and military service legal officers and, according to DOD officials, they are considering conducting required refresher training for SARCs.

Development of Processes for Monitoring the Completeness of Data

DOD and each of the military services have developed processes for monitoring the completeness of data input into DSAID. The primary tool used to monitor DSAID data is DOD's DSAID quality assurance tool. This tool allows users to run point-in-time reports that identify missing data in DSAID; validate the accuracy of selected data fields; and perform cross-checks of selected data fields to identify potential conflicts of information. Officials from each of the services' headquarters-level SAPR offices said that they distribute quality assurance reports monthly to their installations and request that SARCs correct any issues identified before the next monthly report is generated. According to DOD and SAPR officials for two of the military services, these reports allow them to identify trends in data quality issues. SAPR officials for two of the military services also told us that they use quality assurance reports to perform more targeted training to address installation-specific needs. According to DOD officials, data errors identified by the quality assurance tool provides DOD and the military services the opportunity to fix or improve the data entry quality or

[27] "Change control" is a method to formally introduce change requests to a software system and to trace those change requests from initiation to implementation. A "change request" is a formal request to modify the DSAID system or software documentation to correct an error or to accommodate an improvement or any other type of change that is desired by the person making the request.

processes. For example, DOD recently used the quality assurance tool to identify some cases without any subject record. As a result, DOD officials have made plans to meet and develop solutions. Additionally, DOD officials conduct regular manual and automated data validation checks of DSAID to help ensure that sensitive information is protected as well as to help ensure the general integrity of the data. SAPR officials for three of the military services' SAPR offices also told us that they conduct military service-specific reviews of DSAID data on an ongoing basis to help ensure their completeness and accuracy, and to identify any systemic issues.

Users Have Identified Technical Challenges with DSAID and DOD Plans to Implement Modifications to Alleviate Challenges

DSAID users have identified a variety of technical challenges with the system and DOD officials told us they have plans to spend approximately $8.5 million to address most of these issues in fiscal years 2017 and 2018. Some of the key technical challenges users have reported experiencing with the system are related to DSAID's system speed and ease of use; interfaces with MCIO databases; utility as a case management tool; and users' ability to query data and generate reports. DOD has plans in place to implement modifications to DSAID that are expected to alleviate these challenges; however, officials stated that they will not get approval to fund these modifications until after having conducted an analysis of alternatives in line with DOD's acquisition policy framework.[28] This framework, and the GAO Cost Estimating and Assessment Guide[29] outline key elements that should be included in this analysis, such as relative lifecycle costs and benefits; the methods and rationale for quantifying the lifecycle costs and benefits; the effect and value of cost, schedule, and performance tradeoffs; the sensitivity to changes in assumptions; and risk factors for any proposed modifications. DOD plans to complete the first draft of this analysis by the end of November 2016.

[28] Department of Defense Instruction 5000.02, *Operation of the Defense Acquisition System* (Jan. 7, 2015).

[29] GAO-09-3SP.

DSAID Users Have Experienced Technical Challenges That Hinder the Use of the System

Based on our review of the nearly 600 DSAID help desk tickets that were generated from January 2015 through April 2016; DSAID change requests; user feedback reports; interviews with SARCs, program managers, and DOD officials; and our first-hand observations made during visits to selected installations, we identified technical challenges that users reported with DSAID that hinder its use across the military services.[30] These challenges are related to, DSAID's system speed and ease of use; interfaces with MCIO databases; DSAID's utility as a case management tool; and users' ability to query data and generate reports.

- System speed: According to our review of DSAID help desk tickets and interviews with service SAPR officials and SARCs, DSAID's slow system speed presented a challenge in efficient use of the database. Specifically, users report that slow system speed caused them to spend an inordinate amount of time on data input, and limited their ability to save data and run reports because the system is programmed to time out after a certain period. In our review of the DSAID developer's monthly system performance reports from December 2014 through January 2016, we learned that DSAID is rebooted on an almost daily basis to prevent or minimize system slow down. Further, in our review of nearly 600 help desk tickets, we found that DSAID's slow system speed was one of the challenges cited by users. Users reported that, due to issues with system speed, it was cumbersome to perform their required DSAID functions along with other job responsibilities. For example, SARCs we interviewed representing 7 of the 13 installations said that in their estimation, DSAID's slow system speed regularly resulted in data input taking up to two to three times longer than it should have. Additionally, according to interviews with military service officials and SARCs representing 8 of the 13 installations, computers would frequently time out during the lengthy period of time it took to input and save data in DSAID and, if all required fields to save were not complete, the time-out would result in the need to reenter the data. In addition, officials from the Department of the Army told us they were unable to run all-

[30] We met with 42 SARCs representing four of the military services that were located at13 installations in the United States. Specifically, we visited 9 installations— Joint Base Langley-Eustis, Virginia; Naval Station Norfolk, Virginia; Goodfellow Air Force Base, Texas; Fort Hood, Texas; Naval Base San Diego, California; Naval Base Coronado, California; Marine Corps Air Station Miramar, California; Marine Corps Base Quantico, Virginia; and Fort George G. Meade, Maryland. At these locations, SARCs representing the following 4 installations were in attendance as well: Marine Corps Base Camp Pendleton, California; Marine Corps Recruit Depot San Diego, California; Presidio of Monterey, California; and Naval Base Point Loma, California.

Army reports during the last half of 2015 because DSAID would time-out before a full report could be generated. Therefore, according to DOD SAPRO officials, they ran the Army's reports for them on a regular basis, and in February 2016, they resolved this immediate issue by implementing a report scheduler capability in DSAID. According to DOD SAPRO officials, this capability allowed the Army and the other military services to run the full report without timing out. DOD SAPRO officials acknowledge the latency issue overall and are addressing it with software and server upgrades that are designed to reduce page load time and ease the burden of data entry on SARCs. DOD SAPRO officials stated that the software upgrades are scheduled for completion in December 2016 and server upgrades in early 2017, but DOD officials emphasized that when DSAID users experience DSAID slow system speeds it can also be an issue with the user's local network, and not with DSAID.

- Ease of use: DSAID users we interviewed and DOD documents that we reviewed cited the inability to easily navigate DSAID as a challenge. According to a DSAID user feedback report, in 2015 the biggest issue SARCs reported to their military service headquarters officials was that the DSAID user interface and navigation could be improved. This was supported by SARCs we met with from 7 of the 13 installations who said that it is easy to miss or skip data fields and pages because the logic flow from one page to the next in DSAID is not intuitive, often leaving those SARCs unsure of how much progress they have made in completing a case record. For example, during our site visit to one installation, we observed instances in which the selection of certain data elements would trigger other data fields that needed to be completed, but the system did not prompt the user that additional data were required. Additionally, Army headquarters officials raised concerns with DSAID's ease of use, stating that improvements to the system's flow would increase data accuracy by ensuring that users enter relevant information when a case was initiated and also decrease the frequency that "relevant data missing" is noted in DOD's annual report. However, DOD officials stated that they are limited in their ability to make some changes to DSAID's workflow because DSAID is a commercial-off-the-shelf system, which does not allow for such customization.[31]

- Automated interfaces with military service investigative databases: Based on DSAID quality assurance tool reports generated by the military services for the first three quarters of fiscal year 2016 and discussions we had with DSAID users, we found that DSAID data that are populated through interfaces with MCIO databases vary in completeness. According to military service officials and SARCs, this is because MCIO data systems are not required to capture the same information that is required for DSAID. For example, an official from one MCIO said that investigators are not required to complete the data field in their database for whether alcohol was used by the subject or victim; however, this same data field in DSAID is designed to be populated automatically with data from the MCIO databases. Further, in September 2014, DSAID was modified to address technical issues with the interface by allowing SARCs or program managers to manually enter these data in instances where MCIO data are regularly omitted. However, according to DOD officials, any additional data received from the MCIOs during the weekly interface will overwrite what the SARC or program manager has entered as the MCIO is the authoritative source for such data.
- Utility as a case management tool: According to DOD documents, DSAID is intended to be a case management tool, and according to DOD's Fiscal Year 2015 annual report, DSAID enhances a SARC's ability to provide comprehensive and standardized victim case management; however, users of DSAID told us that the system is of limited usefulness for case management. According to the DSAID user manual, the system allows for case management in that it enables a victim's incident and referral data to seamlessly transition between locations or SARCs. While DSAID is DOD's system of record and the only system in which SARCs are permitted to maintain case data, according to headquarter-level officials from the Army, the Navy, and the Air Force, and according to Marine Corps SARCs, DSAID is of limited usefulness to the personnel working with victims. Specifically, officials stated that DSAID does not provide the requisite

[31] "Commercial-off-the-shelf" is a term describing software or hardware that is commercially made and available for sale, lease, or license to the general public and that requires little or no unique government modifications to meet the needs of the procuring agency. DOD is currently considering replacing the commercial-off-the-shelf system it uses for DSAID with a customizable system. According to DOD officials, in November 2016 they will begin evaluating alternatives for replacing DSAID's existing software platform with a customizable system.

functionality, such as the ability to input case notes to manage individual cases. Officials from one service's headquarters-level SAPR office said that this functionality would be helpful in ensuring continuity of victim case management. However, according to DOD SAPRO officials, as of December 2016, a change request to the change control board to add the functionality has not been submitted.

SARCs we met with from 9 of the 13 installations similarly stated that DSAID is missing basic elements of standard case management systems, such as the ability to document victim outreach or record unique incident details that may inform referrals for care or other support services. Further, SARCs we interviewed from 8 of the 13 installations indicated they would, at a minimum, like the ability to document how and when they met with victims to track the level of service victims were provided. DOD officials told us that the decision to limit narrative information in DSAID was by design to protect the victim. According to DOD officials, there is concern that their phrasing of narrative information could inadvertently harm the victim were DSAID data subpoenaed in the course of legal proceedings. Additionally, DOD officials noted that there have not been any change requests made to the change control board for the addition of case management elements to DSAID.

- Data query and reporting: According to DOD officials, DSAID has been used to provide data for congressionally mandated reports, produce ad-hoc queries, facilitate trend analysis, and support program planning analysis and management. However, officials from three services' headquarters-level SAPR offices told us that DSAID's reporting capabilities are limited. As a result, many users told us they have developed their own tools to track sexual assault outside of DSAID. For example, the Army's and the Marine Corps' SAPR offices have each developed "dashboard" systems that use raw data from DSAID to identify specific trends that are useful to their leadership and accessible by SARCs for their military service. Further, SARCs we met with from 11 of the 13 installations told us that they keep informal "databases" or hard copy documents on their cases in order to brief their leadership, because they cannot run ad-hoc queries and reports of cases in DSAID for which they are responsible. According to the SARCs, these trackers duplicate key data points input into DSAID (e.g., victim demographics, type of assault, involvement of alcohol, etc.), but do not include any personally identifiable information.

DOD Officials Have Plans to Modify DSAID in Fiscal Years 2017 and 2018 to Alleviate Most of the System's Technical Challenges, and Plan to Conduct an Analysis of Alternatives of System Changes

According to DOD officials, they have planned to spend $8.5 million in funding for fiscal years 2017 and 2018 for DSAID modifications, which officials stated will allow them to implement specific modifications that should alleviate most of the technical challenges identified by users. See table 2 for a complete list of DOD's initiatives planned for fiscal years 2017 and 2018 and the purpose of these initiatives.

Table 2: Department of Defense's (DOD) Planned Initiatives for the Defense Sexual Assault Incident Database (DSAID) in Fiscal Years 2017 and 2018

Initiative	Purpose
Fiscal year 2017	
Add features to track retaliation data in DSAID	Required by the DOD Retaliation Prevention and Response Strategy.
Develop encrypted file storage mechanism in DSAID	Required (per DOD Instruction 6495.02) to retain for 50 years the Victim Reporting Preference Statement and the DOD Sexual Assault Forensic Examination Report for restricted and unrestricted report cases.
Implement pending and approved Change Control Board requests to DSAID	Implement changes that will, among other things, support congressional requirements and address system challenges experienced by users such as: • capturing additional data for DOD's annual reports to Congress on sexual assault. • improving ease of use by reducing steps in the process to open a case.
Add functionality to the enhanced reporting capability	Improve DSAID's system speed, user ability to generate ad-hoc reports, and analytical capabilities.
Implement or update interfaces between DSAID and the service investigative agency systems (for the Army, the Air Force, the U.S. Coast Guard, and the Department of the Navy)	Implement DSAID's interface with the Coast Guard Investigative Agency's system, improve the way that investigative data are transferred to DSAID, and improve the accuracy of these data.
Fiscal Year 2018	
Add business intelligence tools to the enhanced reporting capability module in DSAID	Continue to enhance DSAID's analytical capabilities.
Implement or update interfaces between DSAID and the services' legal agency systems (for the Army, the Air Force, the U.S. Coast Guard, and the Department of the Navy), DOD personnel systems, and external databases (e.g., Defense Management Data Center/ Defense Enrollment Eligibility Reporting System.)[a]	Increase and enhance the ability for DSAID data to be populated through pre-existing data systems to improve data accuracy.
Incorporate additional approved and pending DSAID change requests	Implement changes that will, among other things, support congressional requirements and address system challenges experienced by users.
Migrate to a new government- approved database server	Upgrade certain components within DSAID that will reach end of life and update DSAID's web server software components to increase performance.

Source: GAO analysis of DOD documents.| GAO-17-99

[a]The Department of the Navy's investigative and legal data systems also include data on sexual assaults involving members of the Marine Corps.

DOD plans to spend $3.59 million in fiscal year 2017 and $4.916 in fiscal year 2018 for specific modifications to DSAID to support these initiatives, and officials are in the process of beginning to conduct a formal analysis to identify the costs and benefits of alternative options for implementing each modification. (See app. I for a list of modifications to DSAID that DOD plans to implement to support the initiatives in fiscal year 2017.) For example, a DOD official stated that DOD plans to implement an encrypted file storage mechanism for DSAID, but they have not yet determined how they plan to do this. Rather, this DOD official stated that the analysis of alternatives will establish options for this mechanism and weigh the costs and benefits. This DOD official also stated that the Defense Human Resources Activity—which is responsible for funding DSAID—will not approve DOD to spend resources on the individual modifications until an analysis of alternatives addressing each modification is conducted. According to this DOD official, the initial draft of this analysis will be completed by the end of November 2016, and all planned modifications can be implemented within the planned available budgetary resources. DOD officials based these budgets on rough-order-of-magnitude cost estimates that were derived from costs they have experienced in recent years. For example, costs for adding a module in DSAID to document reports involving retaliation were based on DOD's costs for building DSAID's legal officer module, which was purchased in 2013.The GAO Cost Estimating and Assessment Guide states that rough-order-of-magnitude estimates are useful to support "what-if" analyses and can be developed for a particular phase or portion of an estimate, but unlike an analysis of alternatives, they do not rise to the level of analysis recommended by best practices to support an investment decision and are not considered budget-quality estimates.[32]

In addition to DOD acquisition requirements, an analysis of alternatives is supported by the GAO Cost Estimating and Assessment Guide.[33] These documents identify key elements that should be included in this analysis. For example, an organization should identify relative lifecycle costs and benefits; methods and the rationale for quantifying the lifecycle costs and

[32] GAO-09-3SP.

[33] Department of Defense Instruction 5000.02, *Operation of the Defense Acquisition System* (Jan. 7, 2015); GAO-09-3SP.

benefits; the effect and value of cost, schedule, and performance tradeoffs; sensitivity to changes in assumptions; and risk factors. Further, according to GAO guidance, a comparative analysis of alternatives is essential for validating decisions to sustain or enhance a program. Because these elements are part of DOD's acquisition requirements, if DOD's analysis of alternatives complies with these requirements, it should incorporate these key elements.

Conducting a comparative analysis of alternatives, including identifying and quantifying lifecycle costs and benefits and weighing the cost, schedule, and performance tradeoffs, is key to ensuring that DOD appropriately manages its modifications to DSAID. In 2010, we found that DOD had failed to demonstrate adherence to these key elements in the initial development and implementation of DSAID.[34] By the end of fiscal year 2018, DOD spending on DSAID will exceed initial cost estimates by over $13 million. In 2010, we reported that DOD estimated development and implementation of DSAID to cost $12.6 million, but DOD's estimate did not include costs for program management or sustainment and for lifecycle costs such as operations and maintenance.[35] In December 2012, DOD documentation shows that DOD had adjusted its estimate to $17.9 million to reflect research and development costs for fiscal years 2011 and 2012 and operations and maintenance costs for fiscal years 2013 through 2018. DOD projected it will have spent a total of approximately $31.5 million as of November 2016 on implementing and maintaining DSAID through fiscal year 2018.[36] This is approximately $13 million more than the revised 2012 estimate. If DOD conducts an accurate and complete analysis of alternatives, it should result in more precise cost estimates for planned enhancements. DOD's plan to conduct an analysis of alternatives that adheres to the department's acquisition framework and adequately considers key elements identified in the GAO Cost Estimating and Assessment Guide, as DOD officials have stated that their

[34] GAO-10-215. In 2010, we recommended, in part, that DOD adequately justify investment in the proposed approach on the basis of reliable estimates of life cycle costs and benefits and, as of November 2016, DOD was unable to provide us with evidence that it had ever implemented this recommendation in developing DSAID.

[35] GAO-10-215.

[36] This does not include an additional $22 million that DOD has spent from 2012 through September 2016 on contractors, whose responsibility in part is to conduct data analysis on DSAID data. SAPRO officials were unable to approximate how much of this amount is dedicated to DSAID management and operations, as opposed to other contractor responsibilities.

analysis will do, should position DOD to more accurately assess whether planned modifications to DSAID can be implemented within budget and with the desired outcome.

DOD's Process for Managing Changes to DSAID Substantially Aligns with Key Elements of Industry Standards

DOD manages modifications to DSAID through its change management process, which we found, based on our review of DOD documentation, substantially align with the elements described in the project management and information technology industry standards that we reviewed.[37] "Change management" is the process of controlling changes requested to work products to help ensure that project baselines are maintained.[38] According to the PMBOK® Guide, the activity of change control allows for documented changes within the project to be considered in an integrated fashion while reducing project risk, which often arises from changes made without consideration to the overall project objectives or plans. Configuration management activities can be included as part of an organization's change control process. While change control is focused on managing project change such as identifying, documenting, and approving or rejecting changes to the project documents, deliverables, or baselines, configuration management is typically focused on managing changes to a configuration item or system.[39] Industry standards include descriptions of the following elements of change and configuration management that are applicable to DOD's efforts to manage DSAID: (1) managing change requests; (2) configuration status accounting, tracking and communicating to stakeholders the changes made to the database;

[37] Project Management Institute, Inc., *A Guide to the Project Management Body of Knowledge (PMBOK® Guide) –Fifth Edition* (Newtown Square, Pa.: 2013). PMBOK is a trademark of Project Management Institute, Inc.; IEEE, *IEEE Standard for Configuration Management in Systems and Software Engineering. IEEE Std 828TM-2012* (Revision of IEEE Std 828-2005), March 16, 2012.

[38] Project Management Institute, Inc., *A Guide to the Project Management Body of Knowledge (PMBOK® Guide) –Fifth Edition* (Newtown Square, Pa.: 2013). The PMBOK® Guide defines "baseline" to be the approved version of a work product that can be changed only through formal change control procedures and is used as a basis for comparison.

[39] Project Management Institute, Inc., *A Guide to the Project Management Body of Knowledge (PMBOK® Guide)* –Fifth Edition (Newtown Square, Pa.: 2013). The PMBOK® Guide defines "configuration item" as an aggregation of hardware, software, processed materials, services, or any of its discrete portions, which satisfy an end-use function and whose requirements are specific and designated for separate configuration management. The IEEE standard on configuration management states that configuration items may range from an entire system, including all hardware, software, and documentation, to a single module or a minor hardware component.

(3) interface control, managing the database interfaces; and (4) release management, managing the publication and communication of updates to users.[40]

- (1) Managing change requests: According to the PMBOK® Guide, changes may be requested by any stakeholder involved with the project. Although changes may be initiated verbally, they should be recorded in written form and entered into the change management and/or configuration management systems. Every documented change request—which may include corrective actions, preventive actions, and defect repairs—needs to be either approved or rejected by a responsible individual who is identified in the project management plan or by organizational procedures according to the PMBOK® Guide. When required, the change control process includes a change control board, which is a formally chartered group responsible for meeting and reviewing the change requests and approving, rejecting, or otherwise disposing of those changes and for recording and communicating such decisions. According to the PMBOK® Guide, the roles and responsibilities of this board are to be clearly defined and agreed upon by appropriate stakeholders and documented in the change management plan. Further, the disposition of all change requests, approved or not, are to be updated in the change log that is used to document changes that occur during a project.[41]

  DOD has established a change request process in the DSAID change control management plan and DOD has documented and formally chartered its Change Control Board. The board's roles and responsibilities are defined in the DSAID Change Control Board charter and board members include representation from SAPRO and each military service's SAPR office. Change requests can be

[40] From the IEEE standard on configuration management—configuration management planning and monitoring, configuration change control, configuration identification, configuration auditing, and supplier configuration item control—were outside of the scope of our review because these are functions managed by the DSAID developer. From the PMBOK® Guide, the following inputs, tools and techniques, and outputs were outside of our scope: project management plan and updates to the plan, work performance reports, enterprise environmental factors, organizational process assets, expert judgment, and change control tools. These elements pertain to project management broadly, whereas our scope focused on elements specific to change management.

[41] Project Management Institute, Inc., *A Guide to the Project Management Body of Knowledge (PMBOK® Guide)* –Fifth Edition (Newton Square, Pa.: 2013).

submitted only by board members or their designees. The board meets monthly to evaluate and vote on change requests.

The DSAID Change Control Board charter outlines the requirement that change requests will be captured through a change request form, which will then be uploaded to the board's website and made available to the DSAID community. Both the DSAID Change Control Board charter and the DSAID change control management plan outline DOD's procedures for evaluating these change requests. During its evaluation of each proposed change request, DOD conducts an impact analysis that includes an assessment of the change's potential impact on requirements, development, training, communications, policy, and testing. This impact analysis also assesses the expected level of effort to implement the request. Documentation from the Change Control Board meetings shows that DOD considers approximate costs and time to implement in change request discussions.

DOD also documents and tracks testing and implementation of approved changes in a requirements log. The log includes the approval status, prioritization, and tracking notes for each change request as each moves through the approval process. Once a change request is implemented, DOD updates the requirements log to note which baseline requirement was affected and which system release was included the change. In the requirements log, DOD also documents baseline requirement changes associated with the change requests that have been disapproved and closed.

- (2) Configuration status accounting: According to the IEEE standard on configuration management, the purpose of configuration status accounting is to track the status of configuration items. In this process, organizations track baseline requirements and total changes requested and implemented. This information should provide objective insights into a system's performance overtime and the status of the system as changes are implemented.[42]

  DOD has documented and established baseline requirements for DSAID and, through the change request tracker, DOD tracks total changes requested, implemented, disapproved, deferred, and pending. As previously discussed, DOD conducts an impact analysis of each proposed change request as part of the evaluation process. DOD tracks DSAID's requirements and change requests until release

[42] IEEE, *IEEE Std 828TM-2012*.

and monitors and documents identified defects at each stage until they are resolved, which allows DOD to monitor the system's status as changes are implemented.

- (3) Interface control: According to the IEEE standard on configuration management, organizations use interface controls to manage the interfacing effects that hardware, system software, and other projects and deliverables have on the project. Interface control activities include identifying the product's key interfaces and controlling the interface specifications.[43]

  DOD is currently managing interfaces between DSAID and the MCIO databases to collect sexual assault case information, and DOD plans to incorporate additional interfaces with other DOD systems to collect more case information. DOD documentation shows that the department has identified DSAID's key interfaces and specifications. Specifically, DOD SAPRO has established a memorandum of understanding with each service investigative agency that describe roles and responsibilities and data mapping parameters, which includes a technical description of the fields and types of data that will be interfaced between DSAID and each service investigative agency's system. Through these mechanisms, DOD manages the parameters of these interfaces that provide key information to DSAID. While DOD has met industry standards for identifying key interfaces and controlling interface specifications, as discussed earlier in this report, some DOD users reported some technical challenges with data from the MCIO database interfaces overwriting manually input DSAID data. According to DOD documentation, DOD is taking steps to mitigate them in enhancement efforts, which include improving how investigative data transferred into DSAID, and adding additional database interfaces.
- (4) Release management: According to the IEEE standard on configuration management, release management allows an organization to ensure that the proper deliverables such as changes and fixes to a system are delivered to the designated receiving party, in the designated form, and to the designated location.[44] Release management activities include delivering approved releases and

[43] IEEE, *IEEE Std 828TM-2012.*

[44] IEEE, *IEEE Std 828TM-2012*. A "release" is a version of software or a system under change management that is made formally available to a wider community.

defining the following: a release policy, release planning, release contents, release format and distribution, and release tracking.

In line with defining release policy, DOD's change control board charter defines board members as the authority for establishing DSAID release schedules and prioritize and assign changes to a release. With respect to release planning, we found that DOD has defined the types of releases it delivers and the activities conducted during DSAID's formal release process. DOD has also defined the content, format, and distribution materials to be included in each release. Communication of the release follows a defined process starting with limited distribution to select users and then distribution to the full user community. DOD uses its master project schedule for DSAID to track and monitor release activities.

Agency Comments

We are not making recommendations in this report. We provided a draft of this report to DOD for review and comment. DOD provided technical comments, which we incorporated as appropriate.

We are sending copies of this report to the appropriate congressional committees and to the Secretary of Defense; the Under Secretary of Defense for Personnel and Readiness; the Secretaries of the Army, the Navy, and the Air Force; and the Commandant of the Marine Corps. In addition, the report is available at no charge on the GAO website at http://www.gao.gov.

If you or your staff have any questions about this report, please contact me at (202) 512-3604 or farrellb@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this report. GAO staff who made key contributions to this report are listed in appendix II.

Brenda S. Farrell

Brenda S. Farrell
Director, Defense Capabilities and Management

Appendix I: Change Requests Prioritized for Implementation in Fiscal Year 2017

Table 3 describes change requests to the Defense Sexual Assault Incident Database (DSAID) that the Department of Defense (DOD) has prioritized for implementation in fiscal year 2017. These change requests were approved through DOD's change control process and determined to be priority modifications by the DSAID Change Control Board.

Table 3: Defense Sexual Assault Incident Database (DSAID) Change Requests Prioritized for Implementation in Fiscal Year 2017[a]

Date submitted	Submitted by	Change	Purpose of change
8/2/2013	SAPRO	Modify data field values and data rules to make them consistent with other data field definitions and flow more logically.	Make some of the data elements and data rules more consistent and logical based on the feedback received from testing and user group.
10/10/2013	Army	Add data elements to capture permanent requested expedited transfers.	Meet DOD Annual Report on Sexual Assault in the Military data requirements.
10/16/2013	SAPRO	Modify the process for opening a new case from two screens to one screen.	Reduce confusion regarding the status of a case and whether or not it was created–that is, reducing the confusion created when users generate control numbers after completing only the first screen and therefore not seeing that original cases had already been created.
10/16/2013	SAPRO	Disable major command and supervisory SARC user role from the user registration page due to limited functional access in this user role.	Give users more functional access once switching to SARC user role.
11/7/2013	SAPRO	Review all date fields and their corresponding validation rules, and make the appropriate validation adjustments.	Improve data integrity and increase the accuracy of data reporting.
12/6/2013	Army	Limit the victim and subject unit identification code to six characters.	Promote better data integrity.
12/6/2013	Army	Add email and civilian grade fields to the SARC user registration profile.	Provide an additional contact method that can be used when a SARC cannot be reached by telephone and allow SAPR program managers to ensure that SARCs meet the rank requirements for the position.
12/6/2013	Army	Create a field-based audit log that would contain more information on changes made to a case record in DSAID.	Allow for a more transparent audit trail when multiple SARCs have access to a case due to being assigned the same location code.[a]
12/27/2013	SAPRO	Track victim's voluntary conversion from restricted to unrestricted reporting by renaming the data fields.	Provide a potential metric to count the number of voluntary conversions from restricted to unrestricted reporting to evaluate SAPRO policies and programs.[b]
2/6/2014	Army	Provide an interface with the Defense Enrollment Eligibility Reporting System, Real-Time Automated Personnel Identification System, or an equivalent system.	Provide missing data elements that were not captured or entered by SARCs on victims and subjects, using a quality control process to validate data through the human resources data link for all of the military services, thus eliminating/resolving most of the existing human errors in the system.

Date submitted	Submitted by	Change	Purpose of change
2/10/2014	SAPRO	Allow SARCs to add victim advocates to a case who are not from the same service as the SARC and allow SARCs and program managers to accurately track the service and duty affiliation of victim advocates through queries and reports.	Reduce potential issues with victim advocates when they have permanent changes of station.
4/7/2014	SAPRO	Add "Is High Risk Response Team Activated" to the victim safety page.	Ensure High Risk Response Team assessment is accomplished, if a victim is assessed to be in a high-risk situation.
8/29/2014	Army	Add new, read-only user role to allow command and installation program managers to view DSAID cases being serviced by SARCs within users' assigned locations.	Allow various levels of program managers (e.g., division, corps, etc.) to view information on cases managed by SARCs under their supervision, but not to be able to revise case information or conduct case-level queries to extract detailed information of cases assigned to those SARCs.
8/29/2014	Army	Add new user role, supervisory SAPR program manager.	Support expanded DSAID user access for Army program managers at different levels and add a hierarchy for easier location code assignment for more efficient location code management by service SAPR program managers.
8/29/2014	Army	Add functionality to allow SARC users to run and export reports of cases, without personally identifiable information for their assigned location code.	Allow SARCs to view and manage all of their cases in a single report to increase data integrity by allowing SARCs to run their own quality control check reports and enabling them to view, manage, and report on all of their cases.
11/5/2014	Army	Add MCIO case number and victim identification number to the cross-service report.[c]	Improve the accuracy of identifying duplicate cases entered by other services.
11/5/2014	Army	Provide validation alert of potential duplicate cases to SARCs when they enter a victim's identification number.	Reduce the number of duplicate notifications that are sent to the military services' SAPR program managers after cases are entered and eliminate for the military services' SAPR program managers the time-consuming process of researching each notification, coordinating with multiple SARCs, and ultimately deleting the duplicate case.
11/5/2014	Army	Enhance the "search DSAID case unrestricted" function on the DSAID homepage to include the ability to search for cases by MCIO number and by a subject's last and first name.	Allow SARCs and military service SAPR program managers to find cases more easily during routine searches instead of limiting searches to advanced search queries, which currently only military service SAPR program managers are able to conduct; enable military service SAPR program managers to search for cases by subject, which is particularly useful for PMs when searching for a military subjects and civilian victims; and enable military service SAPR program managers to more easily validate that all valid unrestricted cases investigated by MCIOs are in DSAID.

Date submitted	Submitted by	Change	Purpose of change
12/5/2014	Army	Move victim birth date and gender fields from the victim demographic information page to the DSAID case page.	Increase data accuracy by ensuring that users enter relevant information when initially entering a case.
12/30/2014	Navy	Extend access and visibility of existing sexual assault case management group meeting minutes to SARCs assigned to same location code and to SAPR program managers in DSAID.	Allow for enhanced quality control and accuracy, especially in the event of a SARC vacancy or extended leave.
5/29/2015	Marine Corps	Remove SAFE Kit notification for closed cases.	Reduce notifications to SARCS that do not require any action and eliminate the extra work required by program managers and SARCs to correct a closed case.
6/5/2015	SAPRO	Change categories of subject type for restricted reports.	Reduce confusion when SARCs select subject type for restricted reports. Ensure restricted cases where the subject was Reserve Officer's Training Corps or other non-Academy student will no longer be included in Military Service Academy matrixes.
6/25/2015	Army	Add Reserve Officer's Training Corps rank option for victim and subject pay grade.	Create more accurate reports by distinguishing between military academy cadets and Reserve Officer's Training Corps cadets.
7/7/2015	SAPRO	Add new data element to select the characterization of resignation or discharge in lieu of only in cases where this characterization is the result of the outcome of a court martial case.	Ensure accuracy of characterization of resignations and discharges because the annual report waterfall charts for court-marital outcomes reports the numbers within these categories, but DSAID does not capture this information except in free text case synopsis notes.
7/17/2015	SAPRO	Change all references to DOD Report to the President of the United States on Sexual Assault Prevention and Response to "Metrics" in DSAID and in the data warehouse.	Ensure accuracy because these metrics continue to be used outside the context of the report to the President.
1/27/2016	SAPRO	Add fields to the case synopsis administrative query:	Allow the SAPRO Research and Analysis team to perform efficient analysis on subject disposition and case synopsis analysis and allow the team to identify investigative data in the same administrative query.

Legend: DOD Sexual Assault Prevention and Response Office (SAPRO), Defense Sexual Assault Incident Database (DSAID), Department of Defense (DOD), Sexual Assault Response Coordinator (SARC), Military Service Sexual Assault Prevention and Response Office (SAPR), and Military Criminal Investigative Organization (MCIO).

Source: GAO Analysis of DOD Documents.| GAO-17-99

Note: The modifications were triggered by change requests and were prioritized for implementation in fiscal year 2017. This does not preclude the Department of Defense from implementing additional modifications during this time frame. A "change request" is a formal request to modify the DSAID system and/or software documentation to correct an error or to otherwise accommodate an improvement and any other type of change that is desired by the person making the request. The table does not include change requests submitted by the National Guard and the U.S. Coast Guard.

[a] A "location code" is an 8-digit numeric or alpha code used in DSAID that identifies a location for the purpose of assigning SARCs to primary locations; assigning installation locations for victims; and/or identifying the location of subjects.

[b] "Restricted" reporting allows victims to confidentially disclose sexual assault information to specified individuals. "Unrestricted" reporting allows victims to disclose, without requesting confidentiality or restricted reporting, sexual assault information.

[c] The MCIOs include the following: the U.S. Army Criminal Investigation Command, the Naval Criminal Investigative Service, and the Air Force Office of Special Investigations.

Appendix II: GAO Contact and Staff Acknowledgments

GAO Contact

Brenda S. Farrell, (202) 512-3604 or farrellb@gao.gov

Staff Acknowledgments

In addition to the staff named above, key contributors to this report include Kim Mayo (Assistant Director); Michael Holland; Jim Houtz; Mae Jones; Anh Le; Amie Lesser; Oscar Mardis; Shahrzad Nikoo; Tida Reveley; Monica Savoy; Jasmine Senior; Maria Staunton; and Randall B. Williamson.

Related GAO Products

Sexual Assault: Actions Needed to Improve DOD's Prevention Strategy and to Help Ensure It Is Effectively Implemented. GAO-16-61. Washington, D.C.: November 4, 2015.

Military Personnel: Actions Needed to Address Sexual Assaults of Male Servicemembers. GAO-15-284. Washington, D.C.: March 19, 2015.

Military Personnel: DOD Needs to Take Further Actions to Prevent Sexual Assault during Initial Military Training. GAO-14-806. Washington, D.C.: September 9, 2014.

Military Personnel: DOD Has Taken Steps to Meet the Health Needs of Deployed Servicewomen, but Actions Are Needed to Enhance Care for Sexual Assault Victims. GAO-13-182. Washington, D.C.: January 29, 2013.

Military Personnel: Prior GAO Work on DOD's Actions to Prevent and Respond to Sexual Assault in the Military. GAO-12-571R. Washington, D.C.: March 30, 2012.

Preventing Sexual Harassment: DOD Needs Greater Leadership Commitment and an Oversight Framework. GAO-11-809. Washington, D.C.: September 21, 2011.

Military Justice: Oversight and Better Collaboration Needed for Sexual Assault Investigations and Adjudications. GAO-11-579. Washington, D.C.: June 22, 2011.

Military Personnel: DOD's and the Coast Guard's Sexual Assault Prevention and Response Programs Need to Be Further Strengthened. GAO-10-405T. Washington, D.C.: February 24, 2010.

Military Personnel: Additional Actions Are Needed to Strengthen DOD's and the Coast Guard's Sexual Assault Prevention and Response Programs. GAO-10-215. Washington, D.C.: February 3, 2010.

Military Personnel: Actions Needed to Strengthen Implementation and Oversight of DOD's and the Coast Guard's Sexual Assault Prevention and Response Programs. GAO-08-1146T. Washington, D.C.: September 10, 2008.

Military Personnel: DOD's and the Coast Guard's Sexual Assault Prevention and Response Programs Face Implementation and Oversight Challenges. GAO-08-924. Washington, D.C.: August 29, 2008.

Military Personnel: Preliminary Observations on DOD's and the Coast Guard's Sexual Assault Prevention and Response Programs. GAO-08-1013T. Washington, D.C.: July 31, 2008.

Military Personnel: The DOD and Coast Guard Academies Have Taken Steps to Address Incidents of Sexual Harassment and Assault, but Greater Federal Oversight Is Needed. GAO-08-296. Washington, D.C.: January 17, 2008.

GAO's Mission

The Government Accountability Office, the audit, evaluation, and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through GAO's website (http://www.gao.gov). Each weekday afternoon, GAO posts on its website newly released reports, testimony, and correspondence. To have GAO e-mail you a list of newly posted products, go to http://www.gao.gov and select "E-mail Updates."

Order by Phone

The price of each GAO publication reflects GAO's actual cost of production and distribution and depends on the number of pages in the publication and whether the publication is printed in color or black and white. Pricing and ordering information is posted on GAO's website, http://www.gao.gov/ordering.htm.

Place orders by calling (202) 512-6000, toll free (866) 801-7077, or
TDD (202) 512-2537.

Orders may be paid for using American Express, Discover Card, MasterCard, Visa, check, or money order. Call for additional information.

Connect with GAO

Connect with GAO on Facebook, Flickr, Twitter, and YouTube.
Subscribe to our RSS Feeds or E-mail Updates. Listen to our Podcasts.
Visit GAO on the web at www.gao.gov.

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

Website: http://www.gao.gov/fraudnet/fraudnet.htm
E-mail: fraudnet@gao.gov
Automated answering system: (800) 424-5454 or (202) 512-7470

Congressional Relations

Katherine Siggerud, Managing Director, siggerudk@gao.gov, (202) 512-4400,
U.S. Government Accountability Office, 441 G Street NW, Room 7125,
Washington, DC 20548

Public Affairs

Chuck Young, Managing Director, youngc1@gao.gov, (202) 512-4800
U.S. Government Accountability Office, 441 G Street NW, Room 7149
Washington, DC 20548

Strategic Planning and External Liaison

James-Christian Blockwood, Managing Director, spel@gao.gov, (202) 512-4707
U.S. Government Accountability Office, 441 G Street NW, Room 7814,
Washington, DC 20548