United States Government Accountability Office

Report to Congressional Requesters

February 2019

WEAPON SYSTEM SUSTAINMENT

DOD Needs to Better Capture and Report Software Sustainment Costs

GAO-19-173

GAO Highlights

Highlights of GAO-19-173, a report to congressional requesters

February 2019

WEAPON SYSTEM SUSTAINMENT

DOD Needs to Better Capture and Report Software Sustainment Costs

Why GAO Did This Study

Software is integral to the operation and functionality of DOD equipment, platforms, and weapon systems, including tactical and combat vehicles, aircraft, ships, submarines, and strategic missiles. DOD estimates that software sustainment funding will total at least $15 billion over the next 5 fiscal years. DOD carries out software sustainment at various locations, where DOD uses its maintenance capabilities to maintain, overhaul, and repair its military weapon systems.

GAO was asked to review several issues relating to the sustainment of operational system software for DOD weapon systems. This report examines, among other things, the extent to which (1) DOD has policies and organizations in place to manage the sustainment of operational system software for weapon systems; and (2) DOD and the military departments track costs to sustain weapon system software. GAO reviewed DOD policies and procedures and interviewed cognizant officials from select DOD software centers, among others, who perform weapon system software sustainment activities.

What GAO Recommends

GAO is making five recommendations, including that (1) the Navy categorize and report its software sustainment costs in accordance with DOD policy; and (2) CAPE improve the collection of weapon system software cost data. DOD concurred with GAO's recommendations.

View GAO-19-173. For more information, contact Diana Maurer at (202) 512-9627 or maurerd@gao.gov.

What GAO Found

The Department of Defense (DOD) has policies and organizations to manage the sustainment of operational system software. DOD policy defines software sustainment and software maintenance activities synonymously, to comprise any activities or actions that change the software baseline, as well as modifications or upgrades that add capability or functionality. One example of such an action is the Air Force's modifying the security software on the B-52 bomber to better protect against attempted system penetration. The figure below defines the four categories of software sustainment actions.

The Four Categories of Software Sustainment Actions

Corrective sustainment	Perfective sustainment	Adaptive sustainment	Preventive sustainment
Corrective sustainment activities diagnose and correct software errors after the software is released.	Perfective sustainment activities consist of upgrades to software to support new capabilities and functionality.	Adaptive sustainment activities modify software to interface with changing environments.	Preventive sustainment activities modify software to improve future maintainability or reliability.

Source: DOD Instruction 4151.20, Depot Maintenance Core Capabilities Determination Process (May 4, 2018); National Institute of Standards and Technology. | GAO-19-173

DOD policies on life-cycle management of weapon systems address software sustainment, and several DOD organizations—including DOD software centers—play key roles in overseeing and managing software sustainment. DOD policy includes software maintenance as part of core logistics, and it requires the military departments to report biennially to Congress on their estimated workloads to sustain core logistics capabilities, including estimated costs of these workloads. However, while the Army and Air Force categorize and report software sustainment as part of core logistics, the Navy does not. Without the Navy's categorizing and reporting its software sustainment costs, DOD and Congress are not fully informed of the magnitude and cost of core software sustainment capability requirements. This impedes DOD's efforts to plan for a ready and controlled source of technical competence, and to budget resources in peacetime while preserving necessary surge capabilities.

DOD's ability to track weapon system software sustainment costs is impeded by limitations in its collection of software cost data. First, GAO found that the Office of Cost Assessment and Program Evaluation's (CAPE) Cost and Software Data Reporting system did not collect weapon system cost data from DOD software centers. Recognizing this, CAPE directed in January 2017 that cost and software data efforts on major acquisition programs should begin to be collected from government organizations, including DOD software centers. However, CAPE acknowledges that it lacks an implementation plan to execute and monitor the requirement for these centers to submit cost and software data. Second, GAO also found that the military departments' operating and support cost systems have incomplete software sustainment cost data. DOD policy requires the military departments to collect and maintain actual operating and support costs, including software sustainment costs. Without CAPE's taking steps to prioritize obtaining complete information on operating and support costs for software sustainment, CAPE is challenged in its ability to accurately compile total program costs or provide reliable life-cycle cost estimates to DOD and Congress.

Contents

Letter		1
	Background	5
	DOD Has Policies and Organizations within Weapon System Management and Depot Maintenance to Manage Operational System Software Sustainment	11
	Limitations in DOD's and the Military Departments' Data Reporting Impede DOD's Tracking of Weapon System Software Sustainment Costs	18
	DOD Has Begun Addressing Challenges with Data Rights for Weapon Systems' Software Sustainment but Has Not Yet Reported to Congress on Required Studies	23
	Conclusions	31
	Recommendations for Executive Action	32
	Agency Comments and Our Response	33
Appendix I	Objectives, Scope, and Methodology	34
Appendix II	Select Software Sustainment Activities	40
Appendix III	Comments from the Department of Defense	41
Appendix IV	GAO Contact and Staff Acknowledgments	44
Appendix V	Related GAO Products	45

Tables

Table 1: Department of Defense- (DOD) Reported Fiscal Year 2012, 2014, 2016, and 2018 Estimated Sustainment Costs for Software for the Army, Navy, and Air Force (in millions of dollars)	17
Table 2: Offices Visited or Contacted during Our Review	38
Table 3: Select Software Sustainment Activities	40

Figures

Figure 1: The Four Categories of Software Sustainment Actions 6
Figure 2: Examples of Types of Weapon Systems That Use Software to Support Functionality 7
Figure 3: Milestones and Decision Points in a Typical Acquisition Program 9
Figure 4: Select Department of Defense (DOD) Organizations That Establish and Maintain Software Sustainment Policy and Procedures 14
Figure 5: Information Technology Device to Replace Proprietary Device 26

Abbreviations

CAPE	Cost Assessment and Program Evaluation
CSDR	Cost and Software Data Reporting
DFARS	Defense Federal Acquisition Regulation Supplement
DOD	Department of Defense
DODI	Department of Defense Instruction
MITRE	The MITRE Corporation
NDAA	National Defense Authorization Act
O&S	Operations and Support
OSD	Office of the Secretary of Defense
U.S.C.	United States Code
VAMOSC	Visibility and Management of Operating and Support Costs

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

February 25, 2019

The Honorable John Garamendi
Chairman
The Honorable Doug Lamborn
Ranking Member
Subcommittee on Readiness
Committee on Armed Services
House of Representatives

The Honorable Joe Wilson
House of Representatives

Software is integral to the operation and functionality of Department of Defense (DOD) equipment, platforms, and weapon systems. It has become essential to the capabilities and operations of a vast range of military systems, including tactical and combat vehicles, aircraft, ships, submarines, and strategic missiles. Many weapon systems cannot operate if the software fails to function as required. For instance, errors among thousands to millions of lines of code can result in a mission-critical failure. To keep software on weapon systems functioning properly, DOD maintains and upgrades it throughout the systems' life-cycles. DOD defines software maintenance and software sustainment synonymously, to comprise any activities or actions that change the software baseline of a weapon system, as well as modifications or upgrades that add capability or functionality.[1] This includes requirements development, architecture and design, and integration and testing. Typically, the modification and upgrade activities are performed by teams of government workers, contractor workers, or both. DOD's Future Years Defense Program estimates that software sustainment funding will reach at least $15 billion in total over the next 5 fiscal years.[2]

The DOD Office of Inspector General identified, for fiscal year 2018, several major management challenges. One such challenge is that the Defense Acquisition System often focuses on near-term costs, schedule,

[1]DOD Instruction (DODI) 4151.20, *Depot Maintenance Core Capabilities Determination Process* (May 4, 2018) (incorporating Change 1, Aug. 31, 2018). In this report we refer to both software maintenance and software sustainment activities as software sustainment.

[2]This Future Years Defense Program estimate accounts for military services and defense agencies for fiscal years 2019-2023.

and performance trade-offs to the detriment of long-term costs, even though more than 70 percent of the life-cycle costs of a weapon system are incurred in the system's operating and support phase.[3] However, long-term forecasting of sustainment costs can be difficult.

Our prior work on software sustainment, which dates back nearly four decades, has shown persistent challenges related to the management, cost reporting, and technical data rights of software, among other issues.[4] More recently, our work on the F-35 Joint Strike Fighter program has identified challenges with software development, long-term sustainment funding, and technical data rights.[5] For example, in 2014 we found that delays in developmental flight testing of the F-35's critical software could hinder delivery of the warfighting capabilities the military services expect, and that these delays were due largely to delays in software delivery, limited capability in the software when delivered, and the need to fix problems and retest multiple software versions. As we recommended, DOD conducted an assessment of the specific capabilities that can be delivered and of those that will likely not be delivered to each of the services by their established initial operational capability dates.[6]

[3]DOD Office of the Inspector General Annual Statement, *Top DOD Management Challenges (Fiscal Year 2018)* (Nov. 11, 2017).

[4]GAO, *Mission Critical Systems: Defense Attempting to Address Major Software Challenges*, GAO/IMTEC-93-13 (Washington, D.C.: December 1992); GAO, "Risk and Control of the Software Maintenance Process," *Quality Data Processing* (Washington, D.C.: January 1987); and GAO, *Federal Agencies' Maintenance of Computer Programs: Expensive and Undermanaged*, AFMD-81-25 (Washington, D.C.: Feb. 26, 1981). We did not make any recommendations in the 1992 and 1987 reports. In the 1981 report we made six recommendations regarding development of software maintenance policies and procedures; these recommendations are closed.

[5]GAO- F-35 *Joint Strike Fighter: Development is Nearly Complete, but Deficiencies Found in Testing Need to Be Resolved*, GAO-18-321 (Washington, D.C.: June 5, 2018); GAO- F-35 *Aircraft Sustainment: DOD Needs to Address Challenges Affecting Readiness and Cost Transparency*, GAO-18-75 (Washington, D.C.: Oct. 26, 2017); and GAO- F-35 *Joint Strike Fighter: Problems Completing Software Testing May Hinder Delivery of Expected Warfighting Capabilities*, GAO-14-322 (Washington, D.C.: Mar.14, 2014).

[6]After we issued our report, the Senate Armed Services Committee directed that the Secretary of Defense assess the F-35 program's software development and report to the congressional defense committees on the specific capabilities that will be delivered, and those that will not be delivered, with each service's initial operational capability. On June 22, 2015, the Under Secretary of Defense for Acquisition, Technology, and Logistics issued a Joint Strike Fighter software development report, which met the intent of our recommendation.

You asked us to review several issues relating to the sustainment of operational system software for DOD weapon systems. This report examines the extent to which (1) DOD has policies and organizations in place to manage the sustainment of operational system software for weapon systems; (2) DOD and the military departments track costs to sustain weapon system software; and (3) DOD has addressed challenges securing necessary data rights to sustain weapon system software. Our scope included software sustainment of operational weapon systems.[7]

For objective one, we reviewed DOD policy and organizations in place to manage the sustainment of operational system software. This included DOD Instruction 5000.02, *Operation of the Defense Acquisition System*, which establishes acquisition and life-cycle sustainment policies; and DOD depot maintenance policy, which outlines requirements for DOD materiel maintenance, core requirements, and core sustaining workloads.[8] We also interviewed officials from the Office of the Secretary of Defense (OSD) and the military departments regarding the department's guidance and the processes used to collect the data for DOD's Biennial Core Report. As in our previous reviews of DOD's biennial core reports, we did not assess the reliability of the underlying data provided by the military services for the 2018 DOD Biennial Core Report.[9] However, we determined that the data were sufficiently reliable for the purpose of determining whether the military services had reported costs of workloads in 2012—2018.

We conducted interviews using a semi-structured questionnaire with officials at 11 of 20 DOD depot-level software sustainment activities, also known as DOD software centers, to gain an understanding of how they sustain weapon system software. Although this sample is not generalizable to the population of DOD depot-level software centers, the use of a random sample of software centers helped mitigate any potential selection bias, and the interviews provided valuable information on those

[7]The operations and support phase of the life-cycle in a DOD system begins after full deployment of the system and lasts until the final system ceases operations. DODI 5000.02, *Operation of the Defense Acquisition System* (Jan. 7, 2015) (incorporating Change 3, Aug. 10, 2017).

[8]See DOD Directive 5000.01, *The Defense Acquisition System* (May 12, 2003) (incorporating Change 2, Aug. 31, 2018); DOD Instruction 5000.02; DOD Directive 4151.18, *Maintenance of Military Materiel* (Mar. 31, 2004); and DOD Instruction 4151.20.

[9]See GAO, *Depot Maintenance: DOD Has Improved the Completeness of Its Biennial Core Report*, GAO-19-89 (Washington, D.C., Nov. 14, 2018).

sites selected. The officials we interviewed at DOD software centers included a variety of engineers and others who perform software sustainment activities for weapon system software, including software on air and sea platforms, targeting system software, and communications systems, among others. We interviewed these officials to gain an understanding of policies and procedures they follow to guide their software sustainment activities, how they are organized, and the activities they undertake to sustain the software.

For objective two, we reviewed DOD policy and military department guidance regarding software sustainment cost-reporting requirements, including DOD Manual 5000.04, *Cost and Software Data Reporting (CSDR) Manual*, and applicable financial management regulations.[10] We reviewed the Office of Cost Assessment and Program Evaluation (CAPE) reports to Congress for fiscal years 2016 and 2017 to learn about initiatives that CAPE is taking to improve software cost data reporting. We interviewed officials at select DOD software centers, including officials responsible for weapon system software on several DOD weapon systems, to gain an understanding of how they track cost data. We also interviewed officials from the Office of the Secretary of Defense (OSD), including officials from CAPE, and officials from the three cost analysis agencies responsible for collecting operating and support costs for the military departments' Visibility and Management of Operating and Support Costs (VAMOSC) data collection systems.

For objective three, we reviewed statutory requirements relating to DOD intellectual property and technical data rights to sustain software.[11] We also reviewed the Defense Federal Acquisition Regulation Supplement (DFARS) pertaining to technical data rights.[12] We reviewed DOD policy and guidance, including the *Defense Acquisition Guidebook*.[13] We

[10]See DOD Manual 5000.04, *Cost and Software Data Reporting Manual* (Nov. 4, 2011) (incorporating Change 1, Apr. 18, 2018); DOD Instruction 5000.02; DOD Instruction 5000.73, *Cost Analysis Guidance and Procedures* (June 9, 2015) (Incorporating Change 1, Oct. 2, 2017); and DOD 7000.14-R, *Financial Management Regulation*, Volume 6A, Chapter 14, "Depot Maintenance Reporting" (May 2018).

[11]10 U.S.C. § 2320.

[12]DFARS Subparts 227.71, "Rights in Technical Data," and 227.72, "Rights in Computer Software and Computer Software Documentation."

[13]Defense Acquisition University, *Defense Acquisition Guidebook (*Nov. 2, 2017); and DOD 5010.12-M, *Procedures for the Acquisition and Management of Technical Data* (May 14, 1993).

interviewed officials from OSD, including officials from the Office of General Counsel, military department headquarters, and DOD software centers to gain an understanding of the necessary technical rights to sustain weapon system software, the reasons that technical data rights are needed, and challenges faced by the department. We analyzed select weapon systems for which DOD had complete data rights, as well as weapon systems for which DOD had partial or incomplete data rights, and the actions DOD took for sustainment, such as public-private partnerships. Finally, we reviewed statutory provisions in the fiscal years 2016 and 2018 National Defense Authorization Acts, which directed the Secretary of Defense to commission studies related to DOD intellectual property and establish a cadre of intellectual property experts, and we interviewed OSD officials to understand DOD's status on the provisions. Further details on our objectives, scope, and methodology are presented in appendix I.

We conducted this performance audit from June 2017 to February 2019 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

Overview of Software Sustainment Activities

DOD defines software maintenance and software sustainment synonymously, to comprise any activities or actions that change the software baseline, as well as modifications or upgrades that add capability or functionality.[14] For example, software sustainment activities involve the correction of software errors after the software is released and adaptations to enable interfacing with changing environments. The four categories of software sustainment actions are defined in figure 1 below.

[14]DOD Instruction 4151.20. The Department of the Navy does not concur with this definition, as we discuss later in this report.

Figure 1: The Four Categories of Software Sustainment Actions

Corrective sustainment	Perfective sustainment	Adaptive sustainment	Preventive sustainment
Corrective sustainment activities diagnose and correct software errors after the software is released. For example, corrective sustainment was performed on the Joint Tactical Terminal's Integrated Broadcast Service system software by fixing errors identified in Information Assurance Vulnerability Assessments submitted by users in the field.	**Perfective sustainment activities consist of upgrades to software to support new capabilities and functionality.** For example, perfective sustainment was performed on the B-52 bomber software as part of the B-52 Modernization program by editing the host based security system which prevents intruders and enabled system administrators to identify attempted system penetrations.	**Adaptive sustainment activities modify software to interface with changing environments.** For example, adaptive sustainment was performed on the Command Post of the Future system software by making it compatible with the Windows 10 Operating System.	**Preventive sustainment activities modify software to improve future maintainability or reliability.** For example, preventive sustainment was performed on Command Post of the Future program by analyzing system software and reducing install and configuration time.

Source: DOD Instruction 4151.20, Depot Maintenance Core Capabilities Determination Process (May 4, 2018); National Institute of Standards and Technology. | GAO-19-173

A software sustainment activity can be categorized in multiple areas. For example, an Army command is modifying software to incorporate Windows 10. This action may be described as corrective in that it addresses errors in previous versions of Windows; perfective in that it upgrades the software to support new capabilities and functionality provided by Windows 10; adaptive in that it can accommodate changes to firmware and hardware environments; and preventive in that it improves reliability.[15]

Sustaining software is normally different from sustaining hardware. For example, when hardware breaks, technicians can remove the broken part—such as tread on a tracked vehicle— and install a working part. In contrast, sustaining software typically requires writing, testing, and deploying lines of code. Software provides critical functionality to nearly every hardware system that DOD uses: surface (for example, mobile network systems); air (for example, secure communications arrays in aircraft); sea (for example, submarine guidance systems); missile (for example, targeting systems); ordnance (for example, Common Remotely Operated Weapon Station); and space (for example, positioning software), as shown in figure 2.

[15]See appendix II for further examples of software sustainment activities that fall into multiple categories.

Figure 2: Examples of Types of Weapon Systems That Use Software to Support Functionality

Device		Software is...
	Surface fixed	At a fixed site
	Surface mobile	Moved somewhere and set up
	Surface portable	In a handheld device
	Surface vehicle	Embedded as part of a moving ground vehicle
	Air vehicle	Embedded as part of an aircraft
	Sea system	Embedded as part of a surface or underwater boat/ship
	Missile system	Embedded as part of a missile system
	Ordnance system	Embedded as part of an ordnance system
	Space system	Embedded as part of a spacecraft

Source: GAO analysis of Department of Defense information. | GAO-19-173

Further, a weapon system may comprise numerous software systems, each supporting different components of the system. Hundreds, or even thousands, of software systems can be embedded in a single weapon system. Interoperability and integration within the weapon system as a whole constitute key software considerations for the overall weapon system's sustainability. For example, the military departments include system-of-systems and family-of-systems considerations. These considerations are defined as a set or arrangement of systems that results when independent systems are integrated within a larger system that delivers unique capabilities. Missions are performed by a system-of-systems arrangement of the platforms and systems that deliver the mission capability.

Weapon System Software and the Acquisition Life-Cycle

Decisions affecting the software on a weapon system are made throughout the acquisition life-cycle. The life-cycle is outlined in DOD Instruction 5000.02, *Operation of the Defense Acquisition System*. This instruction includes four basic and two hybrid models that serve as examples of defense program structures. The hybrid models combine models, such as a weapon system development that includes significant software development. The instruction also includes phases and milestones to oversee and manage acquisition programs, including major weapon systems. It outlines considerations affecting software sustainment for each milestone, including, for example, the following:

- Milestone A: The understanding of the technical, cost, and schedule risks of acquiring the materiel solution; the determination of core requirements; and the development of an intellectual property strategy, to include technical data and computer software deliverables. For example, for incrementally deployed software-intensive programs, the preliminary scope of limited deployment is determined for evaluation prior to a full deployment decision for each capability increment.
- Milestone B: A standard series of design reviews performed prior to converging on a final design for production. For example, for a hybrid acquisition program such as the combination of a major weapon system's basic structural hardware development with a simultaneous software-intensive development, criteria establishing maturity for the development of software functional capability are to be identified.
- Milestone C: The point at which a program or increment of capability is reviewed for entrance into the production and deployment phase or for limited deployment. For example, a general criterion applied during review would be to have a mature software capability consistent with the software development schedule.

Figure 3 depicts the milestones and decision points that inform a typical acquisition program.

Figure 3: Milestones and Decision Points in a Typical Acquisition Program

Source: GAO analysis of Department of Defense (DOD) information. | GAO-19-173

Decisions affecting the software of a weapon system are made throughout the acquisition life- cycle and involve stakeholders across a number of domains. For example, DOD officials are involved in software development, architecture and design, engineering, coding, integration and testing, cost estimation and collection, and intellectual property. Many decisions affecting software sustainment, such as software data rights decisions, typically occur in one of the phases prior to operations and support. Decisions made in the early phases may have long-term effects on a weapon system's sustainability, especially for systems that endure beyond their originally intended design life. Software sustainment decisions are often revisited during the operations and support phase, as hardware breaks or needs to be replaced, a new capability or requirement is added, or a modification is made due to feedback received after a weapon system is fielded.

Software Sustainment as Part of Depot Maintenance, Core Requirements, and Core Sustaining Workloads

DOD conducts software sustainment at a variety of depot-level maintenance locations.[16] DOD and military policy refer to these locations variously as DOD depot-level software sustainment activities, Software Engineering Centers, Software Support Activities, and Life-Cycle Software Engineering Centers. For purposes of this report, we will refer to these facilities as DOD software centers.

Section 2460 of title 10 of the United States Code defines depot-level maintenance and repair. This term includes all aspects of software maintenance classified by DOD as of July 1, 1995, as depot-level

[16]"Depot-level maintenance and repair" means material maintenance or repair requiring the overhaul, upgrading, or rebuilding of parts, assemblies, or subassemblies, and the testing and reclamation of equipment as necessary (10 U.S.C. § 2460(a)).

maintenance and repair—regardless of the source of funds for the maintenance or repair, or of the location at which the maintenance or repair is performed. DOD maintains many weapon systems (such as aircraft and ships) and equipment (such as radar) at the depot level because the systems are too complex to maintain exclusively at the unit, or organizational, level.

Section 2464 of title10 of the United States Code requires DOD to maintain a core depot-level maintenance and repair capability that is government-owned and -operated. Maintaining this capability provides a ready and controlled source of technical competence and resources to enable effective and timely response to mobilizations, contingencies, or other emergencies. Additionally, DOD must assign these government-owned and -operated facilities (the depots) sufficient workload to ensure cost efficiency and technical competence during peacetime, while preserving the surge capacity and reconstitution capabilities necessary to fully support the strategic and contingency plans prepared by the Chairman of the Joint Chiefs of Staff.

Data Rights in DOD

The term “data rights” in the DOD context typically refers to the license rights that the department acquires in two types of deliverables: technical data and computer software. These rights are addressed in law, in the Defense Federal Acquisition Regulation Supplement (DFARS), and in DOD guidance.[17] These data rights are defined as follows:

- Technical data: recorded information, regardless of the form or method of recording, of a scientific or technical nature (including computer software documentation).
- Computer software: computer programs, source code, source code listings, object code listings, design details, algorithms, processes, flow charts, and related material that would enable the software to be reproduced, recreated, or recompiled.
- Computer software documentation: owner’s manuals, user’s manuals, installation instructions, operating instructions, and other similar items, regardless of how this documentation is stored, that will explain the

[17]10 U.S.C. §2320 addresses “Rights in Technical Data,” and §2321 addresses “Validation of Proprietary Data Restrictions”; Defense Federal Acquisition Regulation Supplement (DFARS) sections 252.227-7013 and 252.227-7014; and DFARS subparts 227.71 and 227.72.

capabilities of the computer software or provide instructions for using the software.

DOD Has Policies and Organizations within Weapon System Management and Depot Maintenance to Manage Operational System Software Sustainment

DOD has policies and organizations in place within weapon system management and depot maintenance to manage the sustainment of operational system software. We found that DOD has policies for managing the life-cycle of weapon systems, including sustainment; and that DOD policy on depot maintenance and cost also considers weapon system software issues. Several organizations, including the Under Secretary of Defense for Acquisition and Sustainment and DOD software centers, play key roles in overseeing and managing software sustainment. Software sustainment activities are conducted at numerous facilities, including military department software centers, weapon system program management offices, government laboratories or software integration laboratories, and contractor facilities. Additionally, while DOD has defined software sustainment and software maintenance activities synonymously, and it defines these functions as part of depot maintenance, we determined that the Navy categorizes and reports software sustainment differently.

DOD Has Policies for Life-Cycle Management of Major Weapon Systems That Include Considerations for Software Sustainment

DOD has published a directive and an instruction to guide the military departments in life-cycle management of major weapon systems, including considerations relating to software and weapon system sustainability.[18] First, DOD's acquisition publications provide DOD-wide policy and assign responsibilities to OSD and the military departments for executing weapon system development, production, and sustainment. For example, weapon system software considerations, including cost and access to technical data (for example, product specifications) and computer software (for example, source code), are to be included in required documentation, such as the Life-Cycle Sustainment Plan and the Systems Engineering Plan.[19] Regulatory and reporting requirements differ

[18]DOD Directive 5000.01 and DOD Instruction 5000.02.

[19]DODI 5000.02 states that a Life Cycle Sustainment Plan is a strategy that is to be a basis for all sustainment efforts, and that it includes defect tracking for software, an intellectual property strategy, and other metrics to sustain software systems over the system's life-cycle. The instruction provides that a Systems Engineering Plan describes the program's overall technical approach and addresses system integration with existing and approved architecture.

depending on a system's cost and acquisition category. These policies are in accordance with statute directing the Secretary of Defense to issue and maintain comprehensive guidance on life-cycle management.[20]

Second, DOD includes weapon system software considerations in its instruction regarding depot maintenance core capabilities.[21] DOD-wide policy assigns responsibilities to OSD and the military departments for the performance of DOD core depot-level maintenance, including software. DOD policy states that maintenance tasks are performed to restore safety and reliability when deterioration has occurred. These tasks help to ensure military readiness, including mobilization and surge capabilities, to support national defense strategic and contingency requirements. Additionally, DOD policy states that, for inherently governmental and core capability requirements, maintenance programs are to use organic—or DOD personnel, rather than contractors—in accordance with the law.[22] These DOD policies accord with the statute directing the Secretary of Defense to maintain a core depot-level maintenance and repair capability to ensure technical competence in peacetime while preserving the surge capacity necessary to fully support strategic and contingency needs. [23]

Third, DOD includes weapon system software considerations in its cost policy and manuals.[24] These policies assign responsibilities for estimation of costs and collection of costs (including operations and support costs). They also prescribe cost data reporting and software resource data reporting requirements.

[20]10 U.S.C. § 2337(a).

[21]DOD Directive 4151.18 and DOD Instruction 4151.20.

[22]DOD defines "organic" as meaning assigned to and forming an essential part of a military organization as listed in its table of organization for the Army, Air Force, and Marine Corps, and meaning assigned to the operating forces for the Navy. See Joint Chiefs of Staff, Joint Publication 1, *Doctrine of the Armed Forces of the United States* (Mar. 25, 2013) (incorporating Change 1, July 12, 2017).

[23]In accordance with 10 U.S.C. § 2464.

[24]DOD 7000.14-R; OSD CAPE *Operating and Support Cost-Estimating Guide* (March 2014); and DOD Manual 5000.04.

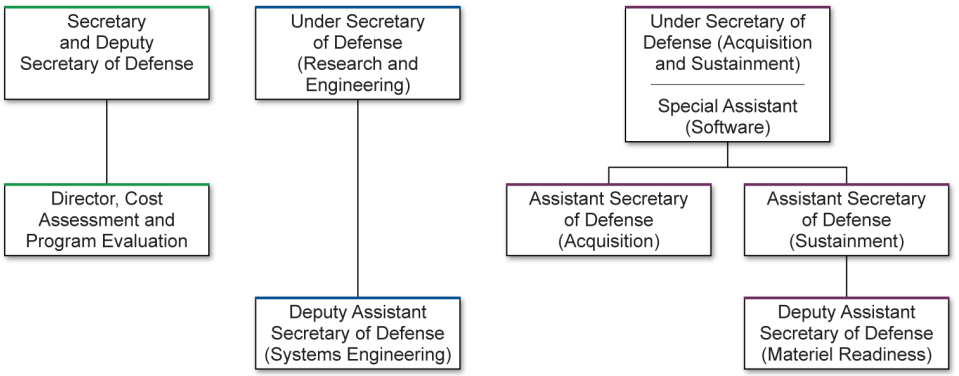
Several DOD Organizations Play Roles in Weapon System Software Sustainment Policy

Several DOD organizations establish policies and procedures for weapon system software sustainment. First, the Under Secretary of Defense for Research and Engineering and the Under Secretary of Defense for Acquisition and Sustainment play key roles in the establishment and maintenance of policy and procedures for software sustainment. For example:

- **Research and Engineering:** This office establishes policy and oversees research, system engineering, and developmental test processes, especially during formative stages of programs. It also supports the Joint Federated Assurance Center, a cross-DOD working group with a mission to develop, maintain, and offer software and hardware vulnerability detection, analysis, and remediation capabilities.
- **Acquisition and Sustainment:** This office establishes policy and manages acquisition and sustainment of major weapon systems. In April 2018 the Under Secretary appointed the first special assistant for software acquisition to advise and assist in addressing software challenges. According to officials, the special assistant will, among other responsibilities, oversee the development of software development policies and standards across DOD practices, and will advise leadership on best practices in software sustainment and data rights issues.

Second, the Deputy Assistant Secretary of Defense for Materiel Readiness, under the Assistant Secretary of Defense (Sustainment), establishes policy for and manages DOD depot-level maintenance, including software sustainment. Third, the Office of Cost Assessment and Program Evaluation analyzes resource allocation and cost estimation, and provides independent analytic advice on, among other things, the cost-effectiveness of defense systems. Figure 4 highlights select organizations that establish and maintain software sustainment policy and procedures.

Figure 4: Select Department of Defense (DOD) Organizations That Establish and Maintain Software Sustainment Policy and Procedures



Source: GAO analysis of DOD policies and guidance. | GAO-19-173

Software Sustainment Activities Are Conducted at DOD Software Centers or Contractor Facilities

Software sustainment is conducted either at DOD software centers—which include military department software centers, weapon system program management offices, government laboratories, and software integration laboratories—or at contractor facilities. The specifics of how the software sustainment is conducted vary by weapon system, in accordance with what the program manager negotiates with the DOD software center or contractor. At DOD software centers, software is developed, tested, and distributed by government staff, contractor staff, or both to maintain operational capability, correct faults, improve performance, and adapt the software to environmental changes. Activities range from small fixes for software errors to large releases that provide weapon systems with new capabilities or address cybersecurity vulnerabilities.

The DOD software centers sustain a range of different systems. For example,

- U.S. Army Communications and Electronic Command's Software Engineering Center sustains software for Army communications systems; and the U. S. Army Aviation and Missile Research Development and Engineering Center sustains software for missiles, space, and aviation;
- The Oklahoma City Air Logistics Complex's 76th Software Maintenance Group at Tinker Air Force Base provides DOD with capabilities in operational flight programs, mission planning systems, space systems, ground-based radar, weapons support, mission

support, jet engine test, training and simulation systems, and diagnostics and repair; and

- Space and Naval Warfare Systems Center Pacific supports and maintains Naval systems in the areas of command and control, communications, computers, and intelligence, surveillance, and reconnaissance, as well as cyber and space.

This work is necessary to maintain and upgrade weapon system software and to meet immediate military operational needs. During our review, officials at DOD software centers provided additional examples of software sustainment activities they conduct on a wide variety of weapon systems. Appendix II provides these additional examples.

DOD Includes Software Sustainment as Part of Depot Maintenance and the Core Logistics Capabilities Determination Process, but Navy's Approach Differs

DOD has defined software sustainment and software maintenance activities synonymously, and it defines these functions as part of depot maintenance and the core logistics process. The Departments of the Army and the Air Force categorize and report software sustainment as part of depot maintenance and the core logistics process. Specifically, the Army and the Air Force have policies that categorize and report software sustainment as part of their core logistics requirements, in accordance with DOD instruction.[25]

Contrary to DOD policy, the Department of the Navy does not categorize and report software sustainment as part of depot maintenance[26] Specifically, Navy officials said that the Navy views software sustainment as an engineering function, not a depot maintenance function. They said that Navy policy reflects the Navy's view of software sustainment as a continuous engineering process that occurs throughout a weapon system's life-cycle, rather than a discrete set of activities categorized as depot maintenance.

These officials stated that while the Navy believes software sustainment to be critical to maintaining its weapon systems, it also believes that managing software sustainment as part of depot maintenance is not the most effective approach for the Navy. In particular, Navy officials

[25]Army Regulation 750-1, *Army Materiel Maintenance Policy* (Aug. 3, 2017); and Air Force Manual 63-122, *Depot Source of Repair Planning and Activation* (May 30, 2017).

[26]The Department of the Navy consists of two services—the United States Navy and the United States Marine Corps.

expressed several concerns about how reporting and categorizing software sustainment as part of depot maintenance could affect their activities. For example, Navy officials noted that this shift would require software engineering to be reported as depot maintenance, which in turn would require the Navy to carry out a greater portion of the work at Navy depots using DOD's workforce. Navy officials stated that, in their opinion, the Navy does not have the capacity to conduct this level of effort with the current DOD workforce within the Navy depot structure, and that the Navy's ability to develop adequate capacity in its DOD software engineering workforce in the future is uncertain. They also stated that shifting this capacity away from private industry to the DOD software engineering workforce could create instability in the management of current and future Navy programs, and would be inconsistent with the Navy's efforts to broaden private-sector software engineering capability and capacity.

We also found that the Department of the Navy does not categorize and report software sustainment as part of its core logistics requirements, in accordance with DOD policy. DOD Instruction 4151.20, *Depot Maintenance Core Capabilities Determination Process*, assigns responsibilities and prescribes procedures to identify required core capabilities for depot maintenance and the associated workloads needed to sustain those capabilities. It is DOD policy that the core capability requirements determination process underpins the establishment and retention of a broad set of public-sector depot maintenance capabilities necessary for DOD, and that the required core capabilities and depot maintenance workloads necessary to sustain those capabilities will be calculated by military services and then aggregated to determine the overall DOD core requirements. As such, DOD requires the military services to use a computational methodology to identify their essential core capability requirements and their planned workload to support this core maintenance capability.[27]

The Navy's differing approach to categorizing and reporting software sustainment has created challenges for DOD-wide reporting on core

[27]According to DOD Instruction 4151.20, a core capability requirement is defined as the depot maintenance capability (including personnel, equipment, and facilities) maintained by DOD at government-owned, government-operated facilities as the ready and controlled source of technical competence and resources necessary to ensure effective and timely response to a mobilization, national defense contingency situation, or other emergency requirement.

logistics capabilities. DOD is required by law to submit a Biennial Core Report to Congress that identifies core logistics capabilities—and DOD has included software sustainment—at depots, and the workload required to maintain those capabilities.[28] The Army and the Air Force included direct labor hours and estimated sustainment costs for DOD depot-level software sustainment in the 2018 DOD Biennial Core Report. However, while the Navy conducted software sustainment activities, it did not consider these activities to be part of depot maintenance or a core logistics capability, as previously discussed. As a result, the Navy reported no direct labor hours or estimated cost of sustaining its software workload for inclusion in the 2018 DOD Biennial Core Report, as shown in table 1. OSD accepted the Navy's core report submission for the 2018 DOD Biennial Core Report.[29]

Table 1: Department of Defense- (DOD) Reported Fiscal Year 2012, 2014, 2016, and 2018 Estimated Sustainment Costs for Software for the Army, Navy, and Air Force

(in millions of dollars)

	Estimated costs of workloads to sustain core requirements – software			
	Fiscal year 2012	**Fiscal year 2014**	**Fiscal year 2016**	**Fiscal year 2018**
Army	33	75	75	232
Navy	3	7	77	0
Air Force	393	451	605	596
Total	**429**	**533**	**757**	**828**

Source: GAO analysis of DOD's 2012, 2014, 2016, and 2018 Biennial Core Reports. | GAO-19-173.

Note: Numbers have been rounded.

The Department of the Navy's position that software sustainment is not part of depot maintenance is contrary to DOD Instruction 4151.20, which specifically includes software sustainment as part of depot maintenance. Without the Department of the Navy's categorizing and reporting of its software sustainment costs, in accordance with DOD policy on the *Depot Maintenance Core Capabilities Determination Process*, DOD and

[28]10 U.S.C. §2464.

[29]Before DODI 4151.20 was updated and reissued in May 2018, OSD obtained input from the military departments and OSD considered issues raised by the Department of the Navy regarding software sustainment. However, OSD made a DOD enterprise-wide decision to move forward with including software sustainment as part of depot maintenance.

Congress are not fully informed of the magnitude and cost of core software sustainment capability requirements for the Navy. Accordingly, DOD is impeded in its efforts to plan for a ready and controlled source of technical competence, and to budget resources in peacetime while preserving the surge capabilities necessary to fully support strategic and contingency needs.

Limitations in DOD's and the Military Departments' Data Reporting Impede DOD's Tracking of Weapon System Software Sustainment Costs

DOD's ability to track weapon system software sustainment costs is impeded by limitations in the collection of software data by both the Office of Cost Assessment and Program Evaluation and the military departments.[30] CAPE oversees the primary cost data collection systems: the Cost and Software Data Reporting system and the military departments' Visibility and Management of Operating and Support Costs system. Further, CAPE has limitations in its cost and software data reporting system for data collected from DOD software centers. We also found that the military departments collect incomplete data on software sustainment costs in their VAMOSC systems.

CAPE Has Limitations in Its Cost and Software Data Reporting System

CAPE collects software sustainment cost data from contractors on certain major weapon systems through its CSDR system. According to CAPE's CSDR manual, this system serves as the primary repository of contractor costs for use in most DOD resource analysis efforts, including cost database development, applied cost-estimating, cost research, program reviews, analysis of alternatives, and life-cycle cost estimates. Data from the two principal components of the CSDR system–contractor cost data reporting and software resources data reporting systems—can be used in managing software sustainment costs. Data in the CSDR system may also be used to prepare acquisition and life-cycle cost estimates for weapon system milestone reviews, as well as to estimate and project software sustainment costs.[31]

We identified limitations, however, in CAPE's CSDR system. First, the system has historically not collected information from contractors for

[30]DOD defines software maintenance and software sustainment synonymously. As previously noted, in this report we refer to both software maintenance and software sustainment activities as software sustainment.

[31]Cost estimating in support of milestone reviews is presented to the Defense Acquisition Board and DOD Component acquisition executive at system milestone reviews.

weapon system acquisition programs whose spending levels did not reach the major defense acquisition program threshold.[32] Although collecting this information was not a requirement in the past, in 2016 Congress directed DOD to begin to collect additional information necessary to facilitate cost estimation and comparison across acquisition programs, including costs from programs with eventual total expenditures greater than $100 million. In February 2018, as part of its overall efforts to make data collection more robust, CAPE issued a memo stating that the Army, Navy, and Air Force proposed pilot programs to collect contractor cost data from 26 weapon system programs whose spending levels were below the major defense acquisition program threshold. CAPE plans to use the results of these pilot programs to inform future efforts to improve information-gathering on, and visibility into, the actual expenditures for lower-dollar programs. Additionally, CAPE plans to update its cost-collection policies and manual, if necessary, upon completion of the pilot programs. Because the department is in the midst of these pilot programs and has outlined next steps to be taken upon their completion, we are not making a recommendation about this matter at this time.

Second, CAPE's CSDR system does not collect any weapon system cost or software data from DOD software centers. Prior to 2017, CAPE required only contractors—and not DOD software centers—supporting major defense acquisition programs to report software sustainment costs into the CSDR system. However, in January 2017 CAPE recognized that the lack of cost and software data from government-executed elements of acquisition and sustainment programs was impeding accurate compilation of total program costs. Accordingly, it issued a memorandum to the military departments directing that cost and software data efforts on major defense acquisition programs should also be collected and submitted into the CSDR system by government-performed efforts, which include DOD software centers. Also, the Standards for Internal Control in the Federal Government states that management should use quality information to achieve an entity's objectives, and that management should obtain data

[32]A Major Defense Acquisition Program is one that is not highly sensitive classified and that is designated by the Secretary of Defense as a Major Defense Acquisition Program or that is estimated by the Secretary of Defense to require eventual total expenditure for research, development, test, and evaluation of more than $480 million (fiscal year 2014 constant dollars) or for procurement of more than $2.79 billion (fiscal year 2014 constant dollars).

from reliable internal and external sources in a timely manner based on the identified information requirements for effective monitoring.[33]

According to a CAPE official, as of September 2018, CAPE had not received any inputs into the CSDR system for DOD-performed software sustainment efforts. CAPE officials told us that compliance with this requirement in the memorandum has been very low, and they attributed this to the absence of an implementation plan. The official said that CAPE is currently in the early stages of evaluating cost data systems—that is, CSDR and the military departments' VAMOSC systems—to determine which is the more effective for use in collecting and submitting cost and software data from DOD software centers. The official acknowledged that after completing this evaluation of the systems, CAPE will develop an implementation plan. However, CAPE is still in the early stages of completing its evaluation. Having a robust implementation plan with time frames for key milestones will be important to executing and monitoring CAPE's actions to improve the reporting of software sustainment costs. Without cost and software data from the DOD software centers, CAPE is challenged in its ability to accurately compile total program costs for program managers, cost estimators, and Congress, among other information recipients.

Military Departments Collect Incomplete Software Sustainment Costs in Operating and Support Cost Systems

CAPE is also responsible for executive oversight of the military department VAMOSC programs. Each military department maintains its own unique VAMOSC system to collect the actual operating and support costs, including software sustainment costs, of fielded major weapon systems.[34] Further, DOD policy requires the military departments to collect and maintain these costs in the cost element structure of CAPE's Operating and Support Cost-Estimating Guide (cost guide) to the greatest extent feasible.[35] The CAPE cost element structure categorizes and

[33]GAO, *Standards for Internal Control in the Federal Government*, GAO-14-704G (Washington, D.C.: September 2014).

[34]According to DOD policy, the VAMOSC systems are the department's preferred data source for use in preparing operating and support cost estimates.

[35]DOD Instruction 5000.73 and OSD CAPE, *Operating and Support Cost Estimating Guide* (March 2014).[36]According to the CAPE cost estimating guide, the software sustainment element excludes the costs of new development or major redesigns that provide new capabilities. However, if the costs of new development or major redesigns that provide new capabilities cannot be isolated, these costs will be considered as part of software sustainment and should be so noted in the estimate documentation.

defines cost elements that cover the range of weapon system operating and support costs, including software sustainment. CAPE's cost guide defines the software sustainment cost element as the labor, material, and overhead costs incurred after deployment to maintain, modify, and integrate software.[36] Further, Standards for Internal Control in the Federal Government states that agencies should use quality information for decision-making and external reporting purposes. Completeness is a key characteristic of quality information, and management uses quality information to make informed decisions and evaluate an entity's performance in achieving key objectives and addressing risks.

However, officials from CAPE and the military departments acknowledged instances of incomplete software sustainment cost-data collection in the VAMOSC systems. For example:

- Army officials told us that while their VAMOSC system has the capability to collect software sustainment cost data, it currently does not capture these data. The Army has undertaken studies examining the costs of software sustainment, and Army leadership acknowledged the need for accurate software sustainment cost estimates, which rely, in part, on the actual historical costs of maintaining the software. Officials told us that to address the lack of software sustainment cost data in the VAMOSC system they are reviewing Army-wide logistics and financial Enterprise Resource Planning systems to determine whether these can serve as automated sources for the needed data. Army cost analysis officials told us that, in the meantime, they plan to start collecting software sustainment cost data from weapon system program offices via a data call and then manually entering the data into the VAMOSC system.
- A Navy official told us that the Navy's VAMOSC system collects some, but not all, weapon system software sustainment costs. For example, according to a Navy cost analysis official, the Navy's VAMOSC system does not contain software sustainment cost data for all shipboard systems. This official explained that no single information technology system includes the software sustainment costs for shipboard systems from program offices across the Navy's

[36]According to the CAPE cost estimating guide, the software sustainment element excludes the costs of new development or major redesigns that provide new capabilities. However, if the costs of new development or major redesigns that provide new capabilities cannot be isolated, these costs will be considered as part of software sustainment and should be so noted in the estimate documentation.

major commands. Therefore, in order to include software sustainment costs for all shipboard systems in the VAMOSC system, Navy officials must manually collect these cost data. This official explained that since the Navy collects these costs manually, officials focus their efforts on the most expensive and most populous shipboard systems. According to the official, they intend to address the Navy VAMOSC system's incomplete software sustainment data issue by expanding their manual data collection efforts to include additional Navy systems.

According to DOD policy, CAPE's executive oversight responsibilities include annually reviewing the services' VAMOSC systems to address data accessibility, completeness, timeliness, accuracy, and compliance with CAPE guidance.[37] CAPE formed a VAMOSC task force in partnership with the service cost-analysis agencies and the Product Support Division in the office of the Assistant Secretary of Defense for Sustainment. The task force is aware of gaps in the military departments' reporting of software sustainment costs within their VAMOSC systems, particularly within the Army and the Navy, and it has included data completeness in the scope of its efforts. However, closing data gaps is not one of the specific purposes of the task force; these purposes include (1) discussing integration of operating and support cost collection across the department and (2) clearly defining the technical differences across the military services' VAMOSC systems.

The task force is concerned with multiple cost-reporting issues. We recognize that the task force can enable DOD to improve the completeness of its software sustainment cost reporting. Further, systematic and institutionalized cost data collection by each military department is important to support credible cost estimates of current and future programs. However, without CAPE taking steps to prioritize obtaining complete information on operating and support costs for software sustainment, it cannot provide reliable life-cycle cost estimates to DOD acquisition or maintenance officials—or Congress— to assist with current and future years funding decisions.

[37]DOD Instruction 5000.73 and OSD CAPE, *Operating and Support Cost Estimating Guide* (March 2014).

DOD Has Begun Addressing Challenges with Data Rights for Weapon Systems' Software Sustainment but Has Not Yet Reported to Congress on Required Studies

DOD Makes Decisions about Securing Data Rights throughout Weapon Systems' Life-Cycles

DOD continuously makes decisions about securing data rights, both early and throughout the life-cycle of a weapon system (see sidebar).

DOD may obtain data rights, including access to technical data and computer software related to weapon systems, for a variety of reasons. For example, as we have previously reported, data rights may be obtained to help control costs and maintain flexibility in future acquisition and sustainment of systems and subsystems, including maintenance and upgrade of weapon system software.[38] DOD officials we spoke with emphasized that there is no one-size-fits-all approach. Further, obtaining data rights for software sustainment constitutes only one of many competing priorities that must be considered along with cost, schedule, and performance in the acquisition of weapon systems.

During the acquisition of a weapon system, DOD makes decisions about the extent of data rights it will acquire. As part of that decision-making process, DOD often negotiates for license rights, and not ownership, of

[38]See appendix V for related GAO products for references to products in which we reported on data rights issues.

Data Rights

The term "data rights" typically refers to the license rights that DOD acquires in two types of deliverables: technical data and computer software. These rights are addressed in law, in the Defense Federal Acquisition Regulation Supplement (DFARS), and in DOD guidance. These data rights are defined as follows:

- Technical data: recorded information, regardless of the form or method of recording, of a scientific or technical nature (including computer software documentation).
- Computer software: computer programs, source code, source code listings, object code listings, design details, algorithms, processes, flow charts, and related material that would enable the software to be reproduced, recreated, or recompiled.
- Computer software documentation: owner's manuals, user's manuals, installation instructions, operating instructions, and other similar items, regardless of how this documentation is stored, that will explain the capabilities of the computer software or provide instructions for using the software.

Source: GAO (10 U.S.C. §2320 addresses "Rights in Technical Data," and §2321 addresses "Validation of Proprietary Data Restrictions"; Defense Federal Acquisition Regulation Supplement (DFARS) sections 252.227-7013 and 252.227-7014; and DFARS subparts 227.71 and 227.72.)

technical data or computer software, to be delivered under a contract.[39] DOD officials told us that this was due to cost and proprietary reasons—that is, the contractor retains ownership of the intellectual property, such as the source code.[40] DOD strives to balance the cost of purchasing the rights against the extent of data rights it expects it will need to maintain and support the system for years into the future. For example, DOD obtains data rights for the following reasons:

- To support its ability to evaluate weapon system design in order to sustain weapon system software.
- To operate and sustain weapon systems under changing technical, operational, and programmatic environments. Sustaining systems requires maintenance manuals, drawings, and parts lists and suppliers, among other things.
- To help ensure having the ability to re-compete acquisition of upgrades and sustainment activities to achieve cost savings. Re-competing requires complete technical data packages that enable the manufacture of data equipment from specification.

During the operating and support phase of a weapon system, DOD may need to reconsider its previous decisions about the extent of data rights it previously acquired. DOD officials we spoke with emphasized that there are situations in which the data rights needed may not be known until years into sustainment. A senior-level DOD official told us that it would be useful if data rights could have a pre-negotiated price and be an option as part of the initial contract. Such an option would give the government the right, but not the obligation, to purchase the data rights at the pre-negotiated price if needed, in the future.

[39]The *Defense Acquisition Guidebook* states that data rights for technical data and computer software fall into eight categories, including unlimited rights, government purpose rights, and Small Business Innovative Research data rights, among others. *See Defense Acquisition Guidebook*, chapter 6.

[40]According to the Ninth Edition (October 2018) of Office of the Staff Judge Advocate, Air Force Space and Missile Systems Center, *Acquiring and Enforcing the Government's Rights in Technical Data and Computer Software under Department of Defense Contracts: A Practical Handbook for Acquisition Professionals*, the owner of technical data or computer software has exclusive control over the use, release, and disclosure of that intellectual property (including the right to exclude others from using the technical data or computer software). In contrast, a licensee is limited to using that technical data or computer software in accordance with the terms and conditions of the license the owner has granted the licensee.

DOD Faces Challenges with Data Rights and Has Initiated Steps to Mitigate Them

DOD has faced challenges in securing the necessary data rights to sustain weapon system software. Specifically, having either partial or incomplete data, or unclear data rights, or both can impede the government's ability to support the weapon system as intended. For example, our recent work on the F-35 Joint Strike Fighter Program found that DOD has not defined all of the technical data it needs from the prime contractor, and at what cost, to enable competition of future sustainment contracts.[41]

Officials at DOD software centers told us that they take steps to mitigate challenges posed by having either partial or incomplete data, or unclear data rights, or both for decades-old weapon systems and new acquisitions. For decades-old weapon systems, officials at some DOD software centers stated that they use public-private partnerships to bridge gaps for systems that lack access to the necessary data rights.[42] For example, an Air Force official at Robins Air Force Base told us that the C-5 software sustainment workload has been successful due to a public-private partnership involving the C-5 System Program Office, the 402nd Software Maintenance Group, and the contractor. As part of this partnership, a C-5 software integrated laboratory was established at Robins Air Force Base for DOD personnel to perform software sustainment activities, including deficiency report investigations and testing. In doing so, the 402nd Software Maintenance Group supports $8.4 million in annual C-5 software sustainment requirements.

Officials at DOD software centers further explained that they have the expertise to optimize software that is transferred from a contractor to a DOD software center or to reverse-engineer software for weapon systems, if needed. In some cases, for example, a contractor may decide that it is no longer profitable or advantageous to continue performing the software sustainment; the activities can then be transferred to a DOD software center. Air Force officials at the 402nd Software Maintenance Group stated that on many occasions they have worked to take over

[41]GAO- F-35 *Aircraft Sustainment: DOD Needs to Address Challenges Affecting Readiness and Cost Transparency*, GAO-18-75 (Washington, D.C.: Oct. 26, 2017).

[42]A public-private (i.e. government-industry) partnership is a cooperative arrangement between an organic product support provider and one or more private-sector entities to perform defense-related work, utilize DOD facilities and equipment, or both. Other government organizations, such as program offices, inventory control points, and sustainment commands, may be parties to such agreements.

software from a contractor without any transition period. In 2013 this DOD software center assumed sustainment responsibility from a contractor without any transition period for a radar system on the F-15 aircraft in order to maintain and upgrade its software. After assuming sustainment responsibility, according to an Air Force official, this DOD software center corrected latent defects and added new capabilities to adapt the radar to a changing threat environment.[43] According to the official, this occurred because the contractor shifted focus to newer radar systems. Further, the contractor priced the support for the older radar system above what the Air Combat Command had budgeted for the updates.

Officials at some DOD software centers told us that if they have the source code but do not have the computer software documentation—such as manuals or instructions—they may need to reverse-engineer the software. For example, engineers at U.S. Army Research, Development and Engineering Command, Armament Research, Development, and Engineering Center (ARDEC) reverse-engineered a key software function, as shown in figure 5 below.

Figure 5: Information Technology Device to Replace Proprietary Device

Engineers at U.S. Army Research, Development and Engineering Command reverse-engineered a key software function on a warning and reporting system located on a reconnaissance vehicle.

The function was provided by a proprietary information technology device that translated video and data information received from a sensor to a readable format for the controller of the warning and reporting system.

In doing so, they developed software for a government-developed information technology device to replace the expensive proprietary device, at an approximate cost savings of $50,000 per system.

Source: GAO analysis of U.S. Army Research, Development and Engineering Command information; Defense Visual Information Distribution Service (photos). | GAO-19-173

[43]A latent defect refers to a defect that exists at the time of acceptance but cannot be discovered by a reasonable inspection.

For newer acquisitions, DOD has increased the consideration it affords to the potential needs for access to and delivery of data. For example, Air Force officials said that because of past issues with data rights on legacy systems, they had launched an initiative to ensure that program offices use standardized contract clauses (for example, DFARS software data rights) and contract delivery requirements (for example, models, drawings, associated lists, and specifications) for data rights. To illustrate this, an Air Force official told us that the HH60W Combat Rescue Helicopter program committed early in the life-cycle to securing the necessary data rights for a DOD software center in the 402nd Software Maintenance Group to perform the software sustainment activities. The official told us that the Statement of Work requests that the contractor provide the DOD software center with the source code and full technical data package, to include a complete software-supporting documentation package.

DOD Has Begun Establishing Intellectual Property Policy and Experts but Has Not Yet Reported to Congress on Required Studies on Data Rights

Provisions in the fiscal years 2016 and 2018 National Defense Authorization acts (NDAA) directed the Secretary of Defense to commission studies related to DOD intellectual property, establish an intellectual property policy, and establish a cadre of intellectual property experts. In response, DOD is in the early stages of developing intellectual property policy and establishing a cadre of intellectual property experts. Also, DOD has commissioned studies to review its access to intellectual property for DOD weapon systems, including necessary data rights. However, the department has missed some required reporting time frames, and it has not yet reported to congressional defense committees on the studies' findings and recommendations.

Congress Directed DOD to Establish Intellectual Property Policy and Identify a Cadre of Intellectual Property Experts

In the fiscal year 2018 NDAA, Congress directed the Secretary of Defense, through the Under Secretary of Defense for Acquisition and Sustainment, to (1) develop policy on the acquisition or licensing of intellectual property; and (2) establish a cadre of intellectual property experts to help support the acquisition workforce on intellectual property matters, including acquiring or licensing intellectual property.[44] The law did not include a time frame for completion. The department is in the early stages of addressing these statutory provisions.

[44]National Defense Authorization Act for Fiscal Year 2018, Pub. L. No. 115-91, § 802 (Dec. 12, 2017) (*codified at* 10 U.S.C. § 2322).

According to the law, the policy is intended to enable DOD-wide coordination and consistency in strategies for acquiring or licensing intellectual property; to help ensure that program managers are aware of DOD's rights and consider and use best practices early in the acquisition process; and to encourage customized intellectual property strategies based on the unique characteristics for each system. The cadre of experts is intended to ensure a consistent, strategic, and knowledgeable approach to acquiring or licensing intellectual property by providing expert advice, assistance, and resources to the acquisition workforce on intellectual property matters.

While the department is in the early stages of addressing these statutory provisions, senior-level DOD officials have acknowledged a delay in these efforts, primarily due to the department's recent reorganization.[45] DOD officials stated that the details concerning organizational structure, roles, responsibilities, and realignment of resources had to be finalized in order for the newly formed organizations to implement these provisions. Regarding the intellectual property policy, a senior-level DOD official told us that the Office of Strategy and Design, within the Office of the Secretary of Defense, will facilitate the collaboration of stakeholders to assist in developing the intellectual policy, which the Assistant Secretary of Defense (Acquisition) will then issue and oversee. Senior-level DOD officials spoke with us regarding the complexity of developing this intellectual property policy, as it spans the weapon system life-cycle, including research, development, acquisition, and operating and support considerations.

Regarding the intellectual property cadre, a senior-level DOD official told us that the Assistant Secretary of Defense (Acquisition) may house the cadre. As of August 2018 the department had not yet specified details on the potential size or scope of the intellectual property cadre, nor a time frame to guide implementation. Although not required by law,

[45]Effective February 1, 2018, the DOD reorganization directed by the National Defense Authorization Act for Fiscal Year 2017 provided for the restructuring of the Office of the Under Secretary of Defense (Acquisition, Technology & Logistics) . Pub. L. No. 114-328, § 901 (2016) (*codified* at 10 U.S.C. §§ 133a and 133b). The position has been divided into the Under Secretary of Defense for Research and Engineering and the Under Secretary of Defense for Acquisition and Sustainment.

development of a robust implementation plan with time frames for key milestones could help DOD to execute and monitor its actions.[46]

DOD Established a Government-Industry Panel to Review Technical Data Rights, but the Panel Has Missed Deadlines for Reporting to Congress

In the fiscal year 2016 NDAA Congress directed DOD to establish a Government-Industry Advisory Panel to review technical data rights, and to submit its final report and recommendations to the Secretary of Defense not later than September 30, 2016.[47] The panel, comprising members from both the public and private sectors, was to review defense regulations on technical data and proprietary restrictions to ensure, among other things, that DOD does not pay more than once for the same work, and that contractors are appropriately recompensed for innovation and invention, among several other considerations.[48] The law also directs that the Secretary of Defense submit comments or recommendations to congressional defense committees not later than 60 days after receiving the report. DOD established the panel, as legislatively required.

As of November 2018 the panel had submitted its report to DOD but not to Congress. Panel members acknowledged that the panel is late in reporting to the congressional defense committees, and they attributed the lateness to the complexity of the task. Panel members told us that obtaining consensus between DOD and industry has been difficult, in part because of competing interests. For example, panel members discussed balancing DOD's needed ability to upgrade and support weapon systems—which is difficult to forecast 30 to 40 years into the future—with industry's need for a fair return on its intellectual property investments. In November 2018 the panel submitted the report to the Under Secretary of Defense for Acquisition and Sustainment. The report includes 19 recommendations for legislative, regulatory, and policy changes that, according to the panel chairman, recognize and seek to balance the

[46]We have found that the identification of goals and objectives to be achieved by a plan, activities or actions to achieve those results, and milestones and performance measures constitutes a key characteristic of a comprehensive, results-oriented management framework. See for example GAO, *DOD's 2010 Comprehensive Inventory Management Improvement Plan Addressed Statutory Requirements, but Faces Implementation Challenges*, GAO-11-240R (Washington, D.C., Jan. 7, 2011).

[47]National Defense Authorization Act for Fiscal Year 2016, Pub. L. No. 114-92, § 813(b) (Nov. 25, 2015). This section was amended by the National Defense Authorization Act for Fiscal Year 2017 to, among other things, extend the deadline for submission of the panel's report to February 1, 2017, and to direct the panel to submit its report directly to Congress, as well as DOD. (Pub. L. No. 114-328, § 809(f)(3) (Dec. 23, 2016)).

[48]*See* Pub. L. No. 114-92, § 813(b) (2015), as amended by Pub. L. No. 114-328, § 809(f) (2016).

equities of both government and industry. As of November 21, 2018, the panel had not yet transmitted the report to Congress, but the panel Chairman stated that it planned to do so before the end of the month.

DOD Is Late in Reporting to Congress on a 2017 Study on Access to Intellectual Property for Weapon System Sustainment

In the fiscal year 2016 NDAA, Congress directed DOD to contract with an independent entity to review DOD regulations, practices, and sustainment requirements related to government access to and use of intellectual property rights of private-sector firms. The law also directs the Secretary of Defense to submit a report to the congressional defense committees on the findings of the independent entity, along with a description of any actions the Secretary proposed in order to revise and clarify laws, or actions the Secretary may take to revise or clarify regulations, related to intellectual property rights.[49]

In response, DOD contracted with the Institute for Defense Analyses to review the intellectual property for weapon system sustainment. In May 2017 the Institute released its report on access to intellectual property for weapon system sustainment.[50] The report made six recommendations, including that DOD establish or expand existing organizational capabilities within the DOD components (with OSD support) to provide expertise in the acquisition of intellectual property data and rights to program managers throughout their programs' life-cycles, as well as to other staff involved in weapon system acquisition.

However, DOD has not yet submitted its report to the congressional defense committees on the study's findings and recommendations, though it was required to do so by March 1, 2016. OSD officials acknowledged that they are late in reporting to congressional defense committees on the study's findings and recommendations. They attributed the delay to their intent of awaiting the findings and recommendations on technical data rights, if any, of the Government-Industry Advisory Panel, as discussed above. DOD informed the congressional defense committees twice—most recently in January 2018—that the department would consider the recommendations of the Institute for Defense Analyses and those of the Panel collectively, and would provide its recommendations in a single report after receiving the Panel's report. In

[49]National Defense Authorization Act for Fiscal Year 2016, Pub. L. No. 114-92, § 875 (Nov. 25, 2015).

[50]See Institute for Defense Analyses, *Department of Defense Access to Intellectual Property for Weapon Systems Sustainment*, IDA Paper P-8266; May 2017: Alexandria, Va.

this January 2018 update, DOD noted that the Panel expected to complete its report by March 2018. However, the Panel did not complete its report—for which DOD was waiting before responding to the Institute's study—until November 2018. DOD's report to Congress on any actions it might take in response to the study's findings and recommendations could provide insight into whether laws or regulations related to intellectual property rights need to be revised or clarified.

Conclusions

Software is essential to the capabilities and operations of a vast range of military systems, including tactical and combat vehicles, aircraft, ships, submarines, and strategic missiles. DOD has policies and organizations within weapon system management and depot maintenance to manage operational system software sustainment. DOD has defined software sustainment and software maintenance activities synonymously, and the department includes software maintenance as part of depot maintenance core capabilities. However, the Department of the Navy does not categorize or report software sustainment as part of depot maintenance. Without the Department of the Navy's categorizing and reporting of its software sustainment costs, in accordance with DOD policy on the *Depot Maintenance Core Capabilities Determination Process*, DOD and Congress are not fully informed of the magnitude and cost of core software sustainment capability requirements. As such, DOD is impeded in its efforts to plan for a ready and controlled source of technical competence and to budget resources in peacetime while preserving the surge capabilities necessary to fully support strategic and contingency needs.

Limitations exist in DOD's cost and software data reporting system with regard to its obtaining cost data from DOD software centers, as well as in the military departments' operating and support cost systems. These limitations impede DOD's tracking of weapon system software sustainment costs. Without cost and software data from the DOD software centers as well as complete information on the military departments' operating and support costs for software sustainment, CAPE is challenged in its ability to accurately compile total program costs for program managers, cost estimators, and Congress, among other information recipients.

Lastly, while DOD makes decisions about securing data rights both early and throughout the life-cycle of a weapon system, the department faces challenges in balancing the cost of purchasing the rights against the extent of data rights it expects it will need over the life of the system. DOD

has begun taking actions to address these challenges. For example, DOD has commissioned several studies, at congressional direction, to examine DOD's access to and use of intellectual property, including technical data rights and proprietary restrictions. However, Congress has yet to receive two of those studies. Reporting on the findings and recommendations, as well as on any actions DOD may take in response to both studies, would provide insight and would highlight timely issues with technical data rights to keep Congress and DOD informed of government and industry concerns and enable them to use that knowledge in their decision making on weapon systems that may be in operation for decades to come.

Recommendations for Executive Action

We are making five recommendations to the Department of Defense—one to the Secretary of the Navy and four to the Secretary of Defense.

We recommend that the Secretary of the Navy categorize and report the Navy's software sustainment costs, in accordance with DOD policy on the *Depot Maintenance Core Capabilities Determination Process*. [Recommendation 1]

We recommend that the Secretary of Defense ensure that the Director for Cost Assessment and Program Evaluation complete its evaluation and select the most effective system to obtain cost and software data from DOD software centers, and develop an implementation plan that includes time frames for key milestones to execute and monitor the centers' submission of required data. [Recommendation 2]

We recommend that the Secretary of Defense ensure that the Director for Cost Assessment and Program Evaluation takes steps to prioritize the respective military departments' obtaining and reporting of complete operating and support costs for software sustainment through its VAMOSC systems. [Recommendation 3]

We recommend that the Secretary of Defense develop an implementation plan with time frames for key milestones for establishing a cadre of intellectual property experts. [Recommendation 4]

We recommend that the Secretary of Defense submit a report, as required by law, to Congress about the study on access to intellectual property for weapon system sustainment conducted by the Institute for Defense Analyses, along with a description of any actions that the Secretary proposes, or may take, to revise or clarify regulations related to intellectual property rights. [Recommendation 5]

Agency Comments and Our Response

We provided a draft of this report to the Department of Defense for review and comment. DOD provided written comments, which are reprinted in appendix III. In its comments, DOD concurred with our recommendations and stated it has actions underway or plans to take actions in response to all five of our recommendations.

We are sending copies of this report to the appropriate congressional committees and the Acting Secretary of Defense. In addition, the report will be 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) 512-9627 or maurerd@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 IV.

Diana Maurer
Director
Defense Capabilities and Management

Appendix I: Objectives, Scope, and Methodology

This report examines the extent to which (1) DOD has policies and organizations in place to manage the sustainment of operational system software for weapon systems; (2) DOD and the military departments track costs to sustain weapon system software; and (3) DOD has addressed challenges securing necessary data rights to sustain weapon system software. Our scope included software sustainment of operational weapon systems.[1]

For objective one, we reviewed DOD policies and organizations in place to manage the sustainment of operational system software for weapon systems. This included DOD Directive 5000.01 and DOD Instruction 5000.02, which establish acquisition program policies; and DOD Directive 4151.18 and DOD Instruction 4151.20, which outline requirements for DOD materiel maintenance and DOD programs' core capabilities.[2] We reviewed statutory requirements, including 10 United States Code § 2337, which requires the Secretary of Defense to issue and maintain comprehensive guidance on life-cycle management and the development and implementation of product support strategies for major weapon systems.[3] We compared the processes used by DOD and the military departments against those outlined in DOD policy and statute, and against software sustainment activities performed at several DOD software centers. We identified the roles and responsibilities for conducting software sustainment activities among personnel at each level of DOD bureaucracy. We also interviewed officials from the Office of the Secretary of Defense (OSD) and the military departments regarding the department's guidance and the processes used to collect the data for DOD's Biennial Core Report. As in our previous reviews of DOD's biennial core reports, we did not assess the reliability of the underlying data provided by the military services for the 2018 DOD Biennial Core Report. However, we determined that the data were sufficiently reliable

[1]The operating and support phase of the life-cycle in a DOD system begins with full deployment of the system and lasts until the final system ceases operations. DODI 5000.02, *Operation of the Defense Acquisition System* (Jan. 7, 2015) (incorporating Change 3, Aug. 10, 2017).

[2]See DOD Directive 5000.01, *The Defense Acquisition System* (May 12, 2003) (incorporating Change 2, Aug. 31, 2018); DODI 5000.02, *Operation of the Defense Acquisition System* (Jan. 7, 2015) (incorporating Change 3, Aug. 10, 2017); DOD Directive 4151.18, *Maintenance of Military Materiel* (Mar. 31, 2004); DOD Instruction 4151.20, *Depot Maintenance Core Capabilities Determination Process* (May 4, 2018) (incorporating Change 1, Aug. 31, 2018).

[3]10 U.S.C. § 2337.

for the purpose of determining whether the military services had reported costs of workloads in 2012—2018.

We interviewed officials from the Office of the Secretary of Defense (OSD), including within the Office of the Under Secretary of Defense for Research and Engineering and the Office of the Under Secretary of Defense for Acquisition and Sustainment. Using a semi-structured questionnaire, we also interviewed officials from each of the military department headquarters—U.S. Army G4, Air Force Acquisition office, and the Assistant Secretary of the Navy for Research, Development, and Acquisition—to understand policies and organizations in place to manage the sustainment of operational system software for major weapon systems. We also interviewed industry officials, such as from the Center for Strategic and Budgetary Assessments and the Software Engineering Institute at Carnegie Mellon University. We conducted interviews using a semi-structured questionnaire with officials at select DOD depot-level software sustainment activities, also referred to as DOD software centers for the purposes of this report. We used DOD's Fiscal Year 2016 Maintenance Fact Book to select 11 of 20 DOD depot-level software sustainment activities based on several criteria, including (1) military department, (2) weapon system type, (3) geographical location, and (4) random selection.[4] Although this sample is not generalizable to the population of DOD depot-level software centers, the use of a random sample of software centers helped mitigate any potential selection bias, and the interviews provided valuable information on those sites selected. The officials we interviewed at DOD software centers included a variety of engineers and others who perform software sustainment activities for weapon system software on several DOD weapon systems, including air and sea platforms, targeting systems, and communications systems, among others. We interviewed these officials to gain an understanding of policies and procedures they follow to guide their software sustainment activities, how they are organized, and the activities they undertake to sustain the software.

For objective two, we reviewed DOD policy and military department guidance regarding software sustainment cost reporting requirements, including Department of Defense Manual 5000.04, *Cost and Software Data Reporting Manual*, and applicable financial management

[4]DOD, *DOD Maintenance 2016 Fact Book* (2016).

regulations.[5] We reviewed the Office of Cost Assessment and Program Evaluation (CAPE) Reports to Congress for Fiscal Years 2016 and 2017 to learn about steps that CAPE is taking to address challenges. We interviewed officials at the DOD software centers responsible for weapon system software on several DOD weapon systems to gain an understanding of how they track cost data. We also interviewed officials from OSD, including officials from CAPE, and officials from the three cost analysis agencies responsible for collecting operating and support costs for the military departments' Visibility and Management of Operating and Support Costs (VAMOSC) data collection systems. These agencies include Office of the Assistant Secretary of the Army for Cost and Economics, the Air Force Cost Analysis Agency, and the Naval Center for Cost Analysis.

For objective three, we reviewed statutes governing DOD intellectual property, including technical data rights, computer software, and computer software documentation. These statutes included, for example, 10 U.S.C. §2320, "Rights in Technical Data," and 10 U.S.C. §2321, "Validation of Proprietary Data Restrictions." Both of these statutes are implemented, in part, by the Federal Acquisition Regulation and the Defense Federal Acquisition Regulation Supplement (DFARS), which we also reviewed. Specifically, we reviewed DFARS Subpart 227.71, "Rights in Technical Data," and DFARS Subpart 227.72, "Rights in Computer Software and Computer Software Documentation." Both include sections that address DOD definitions of technical data; computer software; and computer software documentation, policy, acquisition, licensure, and delivery rights, among other items.

We also reviewed DOD policy and guidance, including DOD 5010.12-M, *Procedures for the Acquisition and Management of Technical Data*.[6] We reviewed the *Defense Acquisition Guidebook*, which addresses the acquisition and maintenance of technical data rights to sustain and upgrade software on major weapon systems.[7] We also reviewed

[5]See DOD Instruction 5000.02; DOD Instruction 5000.73 *Cost Analysis Guidance and Procedures*, (June 9, 2015) (Incorporating Change 1, Oct. 17, 2017); DOD Manual 5000.04, *Cost and Software Data Reporting (CSDR) Manual* (Nov. 4, 2011)(incorporating Change 1, Apr. 18, 2018); and DOD 7000.14-R, *Financial Management Regulation*, Volume 6A, Chapter 14, "Depot Maintenance Reporting" (May 2018).

[6]DOD 5010.12-M, *Procedures for the Acquisition and Management of Technical Data* (May 1993) (incorporating Change 1, Aug. 31, 2018).

[7]Defense Acquisition University, *Defense Acquisition Guidebook* (Nov. 2, 2017).

guidance put forth on intellectual property strategies, including a checklist arranged by contract phase for key intellectual property management activities and considerations.[8]

We interviewed officials from OSD, including from the Office of General Counsel and the Office of Strategic Design, as well as officials from the military department headquarters, to gain an understanding of the necessary technical rights to sustain weapon system software, the reasons that technical data rights are needed, and challenges faced by the department. We interviewed officials at the DOD software centers covering a variety of DOD weapon systems to gain an understanding of what technical data rights they need for their respective weapon systems, and the ways in which they manage issues they may encounter in which contractors own the technical data. We analyzed select weapon systems for which DOD had complete data and rights, as well as weapon systems for which DOD had partial or incomplete data rights, and the actions DOD took for sustainment, such as public-private partnerships. We also interviewed members of the Government-Industry Panel examining technical data rights and proprietary data restrictions to gain an understanding of necessary data rights for sustaining weapon systems coupled with proprietary concerns from industry. Finally, we reviewed statutory provisions in the fiscal years 2016 and 2018 National Defense Authorization acts, which directed the Secretary of Defense to commission studies related to DOD intellectual property, and we interviewed officials to understand DOD's status on the provisions.[9]

[8]Department of Defense Open Systems Architecture—Data Rights Team Guidance, *Intellectual Property Strategy* (August 2014); Air Force Space and Missile Systems Center, Office of the Staff Judge Advocate, *Acquiring and Enforcing the Government's Rights in Technical Data and Computer Software under Department of Defense Contracts: A Practical Handbook for Acquisition Professionals*, Ninth Edition (October 2018); United States Army Product Data and Engineering Working Group, *Army Data and Data Rights (D&DR) Guide: A Reference for Planning and Performing Data Acquisition and Data Management Activities throughout the DOD Life-Cycle*, 1st Edition (August 2015); and Office of the Under Secretary of Defense For Acquisition, Technology, and Logistics, *Intellectual Property: Navigating through Commercial Waters, Issues and Solutions When Negotiating Intellectual Property with Commercial Companies (Version 1.1)* (Oct. 15, 2001).

[9]National Defense Authorization Act for Fiscal Year 2018, Pub. L. No. 115-91, § 802 (Dec. 12, 2017) (*codified at* 10 U.S.C. § 2322) and National Defense Authorization Act for Fiscal Year 2016, Pub. L. No. 114-92, § 813(b) (Nov. 25, 2015). This section was amended by the National Defense Authorization Act for Fiscal Year 2017 to, among other things, extend the deadline for submission of the panel's report to February 1, 2017. (Pub. L. No. 114-328, § 809(f)).

Table 2 lists the offices that we visited or contacted during our review.

Table 2: Offices Visited or Contacted during Our Review

Department of Defense	• Office of the Under Secretary of Defense for Acquisition and Sustainment • Office of Deputy Assistant Secretary of Defense for Systems Engineering • Office of Assistant Deputy Under Secretary of Defense (Logistics and Materiel Readiness)/Maintenance Policy and Programs • Office of the Chief Information Officer • Office of Strategic Design • DOD Office of the Inspector General • Office of General Counsel
Joint Chiefs of Staff	• Office of the Joint Staff, Command, Control, Communication, and Computers/Cyber Directorate
Department of the Army	• Office of the Assistant Secretary of the Army for Acquisition, Logistics, and Technology • Office of the Deputy Chief of Staff (Logistics) • Office of the Army Chief Information Officer • Army Materiel Command
Department of the Navy	• Office of the Assistant Secretary of the Navy (Research, Development and Acquisition) • The Office of the Deputy Assistant Secretary of the Navy—Expeditionary Programs and Logistics Management • Office of the Chief of Naval Operations • Naval Center for Cost Analysis
Department of the Air Force	• Office of the Deputy Assistant Secretary for Science, Technology, and Engineering • Deputy Assistant Secretary of the Air Force for Logistics and Product Support, Office of the Assistant Secretary of the Air Force for Acquisition • Air Force Cost Analysis Agency
Depot-level software sustainment activities	
Army Depot-Level Software Sustainment Activities	• Armaments Research Development and Engineering Center, Research Development and Engineering Command, Picatinny Arsenal, NJ • Aviation and Missile Research Development and Engineering Center, Aviation and Missile Command, Redstone Arsenal, AL • Communications-Electronics Command Software Engineering Center, Aberdeen, MD • Tank Automotive Research Development and Engineering Center, Tank Automotive Command, Detroit Arsenal, MI
Navy Depot-Level Software Sustainment Activities	• Naval Air Warfare Center-Training Systems Division, Naval Air Systems Command, Orlando, FL • Naval Surface Warfare Center, Naval Sea Systems Command, Dahlgren, VA • Naval Undersea Warfare Center, Naval Sea Systems Command, Newport, RI • Space and Naval Warfare Systems Center Pacific, San Diego, CA
Air Force Depot-Level Software Sustainment Activities	• Ogden Air Logistics Complex, UT • Oklahoma City Air Logistics Complex, OK • Warner Robins Air Logistics Complex, GA

Industry	
	• Center for Strategic and Budgetary Assessments • Software Engineering Institute, Carnegie Mellon University
Weapon system software— sustaining officials	
Department of the Navy	• Battlefield Management System • Tomahawk Missile System • Littoral Combat Ship • System Track Manager/Track Service • Submarine Sonar Systems • Torpedo MK48 • Surface Anti-Submarine Warfare Combat System • USW Ranges • Submarine Combat Control Systems
Department of the Army	• Army Reprogramming Analysis Team • Satellite Communications • Warfighter Information Network-Tactical System • Common Remotely Operated Weapon Station • Striker • Mine-Resistant Ambush Protected Vehicle
Department of the Air Force	• HH60W Combat Rescue Helicopter • F-35 Joint Strike Fighter • Global Hawk Software Activation • Test Program Set • B-2 Stealth Bomber Sustainment • C5 Strategic Transport Aircraft • F15 Eagle

Source: GAO. | GAO-19-173.

Appendix II: Select Software Sustainment Activities

Table 3: Select Software Sustainment Activities

Activity	Reported Example of Activity
"Bug fixes"	Navy Training Support Department software engineers, on site, remedy minor bugs and make minor operational changes for fielded systems. The Army Tank Automotive Research, Development, Engineering Command team validates defects identified in software-trouble or defect reports submitted by soldiers in the field, designs/implements change, verifies solution, and baselines the new release. These reports allow the Tank Automotive Research, Development, Engineering Command software sustainment team to remedy identified bugs and send the remedies to the field updated software. The Air Force software sustainment team at Warner Robins Air Force Base addresses software bugs with its test program set, a tool that enables technicians to diagnose and repair complex items, automate test procedures, and capture software error data.
Cybersecurity fixes/ patches	The Army Communications-Electronics Command writes and applies annual software patches. Users submit Information assurance vulnerability alerts that identify problems for Army software engineers to address. Software sustainers among the Navy program offices respond to the vulnerability alerts through regular software updates issued every 18 – 24 months. The Army Tank Automotive Research, Development, Engineering Command team identifies cyber security issues through the use of software assurance tools. These tools allow the Tank Automotive Research, Development, Engineering Command software sustainment team to proactively respond to vulnerability alerts by analyzing issues, making corrections, applying appropriate patches, and issuing a new release to the fielded software.
Test vulnerabilities	Software sustainers at Warner Robins Air Force Base analyze software code when they change it to ensure that they do not introduce vulnerabilities. They use multiple techniques, tools, and teams, such as the Cyber Resiliency Office for Weapon Systems analysis team. The Army Tank Automotive Research, Development, Engineering Command team goes through extensive testing of the software in the Software Integration Laboratories as well as testing on the vehicles and other platforms. Sustainment engineers make sure that the software meets requirements compliance, defect containment, software safety, and software product quality through software assurance scans, product inspection, and penetration/vulnerability testing. Department of Defense software designers often design systems using pieces of code they identify on the internet. DOD software architects usually, but not always, use vetted libraries. In cases where they do not, developers could inadvertently insert code produced by an adversary country into DOD systems, thereby allowing that country access to DOD systems. Several off-the-shelf applications exist to detect these vulnerabilities.
System Updates	Navy Program offices modify a software system after delivery to correct faults, improve performance, or adapt it to a changed environment. These can include changes or updates to the software code, or development of a new software baseline. Upgrades to operational system software are typically driven by Fleet/Warfighter needs and requirements. Upgrade requirements are usually captured; vetted; and approved through appropriate authorities, including configuration control boards, program offices, and resource sponsors. The Air Force 309th Software Maintenance Group provides critical system updates for military bombers, fighter jets, missile systems, satellite systems, and others. The group provides "cradle-to-grave" system support, encompassing software engineering, hardware engineering, program management, and data management.

Source: GAO analyses of DOD documentation and interviews. | GAO-19-173.

Appendix III: Comments from the Department of Defense

ASSISTANT SECRETARY OF DEFENSE
3500 DEFENSE PENTAGON
WASHINGTON, DC 20301-3500

SUSTAINMENT

FEB 12 2019

Ms. Diana Maurer
Director, Defense Capabilities and Management
U.S. Government Accountability Office
441 G Street, NW
Washington, DC 20548

Dear Ms. Maurer:

This is the Department of Defense (DoD) response to the GAO Draft Report GAO-19-173, "WEAPON SYSTEM SUSTAINMENT: DoD Needs To Better Capture and Report Software Sustainment," dated November 27, 2018 (GAO Code 102118).

Detailed comments on the report recommendations are enclosed.

Sincerely,

Robert H. McMahon

Enclosure:
As stated

GAO DRAFT REPORT DATED NOVEMBER 27, 2018
GAO-19-173 (GAO CODE 102118)

"WEAPON SYSTEM SUSTAINMENT: DOD NEEDS TO BETTER CAPTURE AND REPORT SOFTWARE SUSTAINMENT"

DEPARTMENT OF DEFENSE COMMENTS TO THE GAO RECOMMENDATION

RECOMMENDATION 1: The GAO recommends that the Secretary of the Navy categorize and report the Navy's software sustainment costs, in accordance with DOD policy on the depot maintenance core capabilities determination process.

DoD RESPONSE: Concur. The DoD recognizes that the Department of the Navy's position that software sustainment is not part of depot maintenance is contrary to the statutory definition of depot-level maintenance and repair (10 USC 2460), which includes all aspects of software maintenance, as software sustainment is synonymous with software maintenance (DoD Instruction 4151.20). The Department of the Navy will be directed to categorize and report the Navy's software sustainment costs, in accordance with DoD policy on the depot maintenance core capabilities determination process.

RECOMMENDATION 2: The GAO recommends that the Secretary of Defense ensure that the Director for Cost Assessment and Program Evaluation complete its evaluation and select the most effective system to obtain cost and software data from DOD software centers, and develop an implementation plan that includes timeframes for key milestones to execute and monitor the centers' submission of required data.

DoD RESPONSE: Concur. The Director for Cost Assessment and Program Evaluation will complete its evaluation and select the most effective system to obtain cost and software data from DOD software centers, and develop an implementation plan that includes timeframes for key milestones to execute and monitor the centers' submission of required data.

RECOMMENDATION 3: The GAO recommends that the Secretary of Defense ensure that the Director for Cost Assessment and Program Evaluation takes steps to prioritize the respective military departments' obtaining and reporting complete operating and support costs for software sustainment through its VAMOSC systems.

DoD RESPONSE: Concur. The Director for Cost Assessment and Program Evaluation will take steps to prioritize the respective military departments' obtaining and reporting complete operating and support costs for software sustainment through its VAMOSC systems.

RECOMMENDATION 4: The GAO recommends that the Secretary of Defense develop an implementation plan with timeframes for key milestones for establishing a cadre of intellectual property experts.

DoD RESPONSE: Concur, the Office of the Assistant Secretary of Defense (Acquisition), is actively working to develop an implementation plan with timeframes for key milestones for establishing a cadre of intellectual property experts, as it was directed in previous legislation.

RECOMMENDATION 5: The GAO recommends that the Secretary of Defense submit a report, as required by law, to Congress about the study on access to intellectual property for weapon system sustainment conducted by the Institute for Defense Analyses, along with a description of any actions that the Secretary proposes, or may take, to revise or clarify regulations related to intellectual property rights.

DoD RESPONSE: Concur, the Office of the Assistant Secretary of Defense (Acquisition), is already actively working to develop the report to Congress about the study on access to intellectual property for weapon system sustainment conducted by the Institute for Defense Analyses. It will include a description of actions that the Secretary proposes, or may take, to revise or clarify regulations related to intellectual property rights.

Appendix IV: GAO Contact and Staff Acknowledgments

GAO Contact

Diana Maurer, 202-512-9627 or maurerd@gao.gov

Staff Acknowledgments

In addition to the contact listed above, Sally Newman (Assistant Director), Laura Czohara (Analyst-in-Charge), Steven Bagley, Steven Boyles, Vincent Buquicchio, Amie Lesser, Janine Prybyla, Andrew Stavisky, and Cheryl Weissman made key contributions to this report.

Appendix V: Related GAO Products

GAO- F-35 *Joint Strike Fighter: Development is Nearly Complete, but Deficiencies Found in Testing Need to Be Resolved*, GAO-18-321 (Washington, D.C.: June 5, 2018).

GAO- F-35 *Aircraft Sustainment: DOD Needs to Address Challenges Affecting Readiness and Cost Transparency*, GAO-18-75 (Washington, D.C.: Oct. 26, 2017).

GAO*, Military Acquisitions: DOD Is Taking Steps to Address Challenges Faced by Certain Companies*, GAO-17-644 (Washington, D.C.: July 2017).

GAO- F-35 *Sustainment: DOD Needs a Plan to Address Risks Related to Its Central Logistics System*, GAO-16-439, (Washington, D.C., Apr. 14, 2016).

GAO- F-35 *Joint Strike Fighter: Preliminary Observations on Program Progress*, GAO-16-489T (Washington, D.C.: Mar. 23, 2016).

GAO*, Defense Contracting: Early Attention in the Acquisition Process Needed to Enhance Competition*, GAO-14-395 (Washington, D.C.: May 5, 2014).

GAO- F-35 Joint Strike Fighter: Problems Completing Software Testing May Hinder Delivery of Expected Warfighting Capabilities, GAO-14-322 (Washington, D.C.: Mar. 24, 2014).

GAO- F-35 Joint Strike Fighter: Program Has Improved in Some Areas, but Affordability Challenges and Other Risks Remain, GAO-13-500T (Washington, D.C.: Apr. 17, 2013).

GAO, *Defense Acquisition: DOD Should Clarify Requirements for Assessing and Documenting Technical-Data Needs*, GAO-11-469 (Washington, D.C.: May 11, 2011).

GAO, *Federal Contracting: Opportunities Exist to Increase Competition and Assess Reasons When Only One Offer Is Received*, GAO-10-833 (Washington, D.C.: July 26, 2010).

GAO, *Weapons Acquisition: DOD Should Strengthen Policies for Assessing Technical Data Needs to Support Weapon Systems*, GAO-06-839 (Washington, D.C.: July 14, 2006).

GAO, Defense Management: Opportunities to Enhance the Implementation of Performance-Based Logistics, GAO-04-715 (Washington, D.C.: Aug. 16, 2004).

GAO, *Defense Logistics: Opportunities to Improve the Army's and the Navy's Decision-making Process for Weapons Systems Support*, GAO-02-306 (Washington, D.C.: Feb. 28, 2002).

GAO, *Defense Logistics: Air Force Lacks Data to Assess Contractor Logistics Support Approaches*, GAO-01-618 (Washington, D.C.: Sept. 7, 2001).

GAO, *Test and Evaluation: DOD Has Been Slow in Improving Testing of Software Intensive Systems*, GAO/ NSIAD-93-198 (Washington, D.C.: September 1993).

GAO, *Mission Critical Systems, Defense Attempting to Address Major Software Challenges*, GAO/IMTEC-93-13 (Washington, D.C.: December 1992).

GAO, *Risk and Control of the Software Maintenance Process* (Washington, D.C.: January 1987).

GAO, *Federal Agencies' Maintenance of Computer Programs: Expensive and Undermanaged*, AFMD-81-25 (Washington, D.C., Feb. 26, 1981).