United States Government Accountability Office

Report to Congressional Committees

September 2023

DOD SOFTWARE LICENSES

BETTER GUIDANCE AND PLANS NEEDED TO ENSURE RESTRICTIVE PRACTICES ARE MITIGATED

Accessible Version

GAO-23-106290

GAO Highlights

Highlights of GAO-23-106290, a report to congressional committees

September 2023

DOD SOFTWARE LICENSES

Better Guidance and Plans Needed to Ensure Restrictive Practices Are Mitigated

Why GAO Did This Study

Cloud computing enables on-demand access to shared computing resources. As DOD implements IT projects and migrates systems to the cloud, it may encounter restrictive software license practices. These practices include enterprise agreements or vendor processes that limit, impede, or prevent agencies' efforts to use software in cloud or multi-cloud computing.

The House report accompanying the James M. Inhofe National Defense Authorization Act for Fiscal Year 2023 includes a provision for GAO to review the impact that restrictive software licensing practices could have on DOD cloud computing. The objectives of this review were to (1) describe how restrictive enterprise software licensing practices impact DOD cloud computing services and (2) evaluate the extent to which DOD is mitigating the potential impact of restrictive software licensing practices.

GAO selected three DOD components (the Army, Air Force, and Navy) with the largest cloud budget requests for fiscal year 2023 and interviewed IT and acquisition officials from these components to describe the impacts of restrictive software licensing practices. GAO also selected six investments based on several factors, including IT budget size, and compared DOD documentation to key activities for mitigation identified by industry.

What GAO Recommends

GAO is making one recommendation to DOD to fully address identifying, analyzing, and mitigating the impacts of restrictive software licensing practices. The department concurred with the recommendation.

View GAO-23-106290. For more information, contact Carol Harris at 202-512-4456 or HarrisCC@gao.gov.

What GAO Found

Officials from all three selected Department of Defense (DOD) components and two of the six selected investments described restrictive software license practices that impacted their cloud computing efforts. Officials from the selected components and investments stated that restrictive practices generally impacted the (1) cost of cloud computing, (2) choice of cloud service providers, and (3) other related impacts. The table provides examples of each of these types of impacts.

Examples of Reported Restrictive Software License Practices by Selected Department of Defense (DOD) Components and Investments

Impact type	Impact description
Cost of cloud computing	Infrastructure costs increased because vendors required additional fees to use their software with third party cloud service providers.
	Licensing costs increased because a vendor bundled frequently used software with other software, making it available only at the bundled price.
Choice of cloud provider	A vendor limited its use to only selected commercial cloud service providers.
	A vendor required a specified cloud service provider.
Other	Vendors required interoperability with a previous version of a different vendor's software, but that vendor does not allow customers to use the previous version unless they are using its cloud service platform.
	A vendor may not help sustain a certain product if a customer is not using the specified cloud service provider.

Source: GAO analysis of data reported by selected Department of Defense components and investments. | GAO-23-106290

Four of the six selected investments did not identify impacts from restrictive software licensing practices. According to officials, they may not have had impacts because these investments were configured to deploy software within the cloud instead of transferring software to the cloud.

Key industry activities for managing the risk of impacts from restrictive practices include (1) identifying and analyzing impacts and (2) mitigating those impacts. However, the six selected investments GAO reviewed did not consistently address these key activities. Specifically, two investments identified an impact but did not analyze or develop plans for mitigating it, while four other investments did not address identifying, analyzing, or mitigating. The lack of relevant guidance allowed these shortfalls to occur. DOD's guidance and plans do not fully address identifying and analyzing the impacts of restrictive practices. Moreover, DOD's plans and guidance do not address mitigating impacts of restrictive practices. Until DOD updates and implements guidance and plans for managing the impacts of restrictive software licensing practices, the department will not be well-positioned to identify and analyze the impact of such practices or to mitigate the risks.

Contents

Why GAO Did This Study ii
What GAO Recommends ii
What GAO Found ii

Letter 1

Background 5
Selected DOD Entities Reported Various Impacts of Restrictive Software Licensing Practices 14
DOD Had Gaps in Guidance and Plans for Mitigating Impacts of Restrictive Software Licensing Practices 16
Conclusions 22
Recommendation for Executive Action 22
Agency Comments 22

Appendix I: Objectives, Scope, and Methodology 25

Appendix II: Comments from the Department of Defense 29

Accessible Text for Appendix II: Comments from the Department of Defense 30

Appendix III: GAO Contact and Staff Acknowledgments 31

Table

Table 1: Impacts of Restrictive Software Licensing Practices Encountered by Selected Department of Defense (DOD) Components and Investments 15

Abbreviations

CIO	Chief Information Officer
DOD	Department of Defense
ESI	Enterprise Software Initiative
NIST	National Institute of Standards and Technology
OMB	Office of Management and Budget
SNaP-IT	Select and Native Programming–Information Technology

This is a work of the U.S. government and is not subject to copyright protection in the United States. The published product may be reproduced and distributed in its entirety without further permission from GAO. However, because this work may contain copyrighted images or other material, permission from the copyright holder may be necessary if you wish to reproduce this material separately.

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

September 12, 2023

Congressional Committees

As part of a comprehensive effort to transform IT within the federal government, in 2010, the Office of Management and Budget (OMB) began requiring agencies to shift their IT services to a cloud computing option when feasible.[1] Cloud computing is a means for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.[2]

In 2018, the Department of Defense (DOD) reported that it managed more than 500 cloud efforts across the department.[3] DOD reported that, between 2021 and 2023, its annual investment in cloud computing services and migration has increased more than 40 percent, from about $1.4 billion in fiscal year 2021 to about $2 billion in fiscal year 2023.[4]

Effectively managing commercial software licenses is a challenge that DOD and other agencies face as they implement IT projects and migrate systems to the cloud.[5] As early as 2012, we reported on the need for agencies to ensure data portability and interoperability as they invested in

[1]Office of Management and Budget, *25 Point Implementation Plan to Reform Federal Information Technology Management* (Washington, D.C.: Dec. 9, 2010).

[2]National Institute of Standards and Technology, *The NIST Definition of Cloud Computing*, Special Publication 800-145 (Gaithersburg, MD: Sept. 2011).

[3]Deputy Secretary of Defense, "DoD Cloud Update," June 22, 2018 memorandum, available at https://federalnewsnetwork.com/wp-content/uploads/2018/07/062218_shanahan_deasy_memo.pdf.

[4]Department of Defense, *Department of Defense Information Technology and Cyberspace Activities Budget Overview, Fiscal Year 2023 Budget Request*, (Washington, D.C.: May 2022).

[5]National Institute of Standards and Technology, *The NIST Definition of Cloud Computing*, Special Publication 800-145 (Gaithersburg, MD: Sept. 2011). Software licenses can be used as part of different cloud service models (e.g., software as a service, platform as a service, infrastructure as a service).

cloud computing.[6] We noted that, to preserve their ability to change vendors in the future, agencies may attempt to avoid platforms or technologies that "lock" customers into a particular product (commonly referred to as vendor lock-in).

House Report 117-397, accompanying the James M. Inhofe National Defense Authorization Act for Fiscal Year 2023, includes provisions for GAO to review the impact that restrictive software licensing practices could have on DOD cloud computing.[7] Our objectives were to (1) describe how restrictive enterprise software licensing practices impact DOD cloud computing services and (2) evaluate the extent to which DOD is mitigating the potential impact of restrictive software licensing practices.

For both objectives, we selected six DOD cloud IT investments[8] from the department's Select and Native Programming–Information Technology (SNaP-IT) database.[9] From that database, we sorted investments based on fiscal year 2023 budget size and grouped the investments into three groups—greater than $100 million, between $100 million and $10 million, and between $10 million and $1 million. We randomly selected an investment from each of the three groups. From the remaining investments, we then randomly selected three additional investments, adjusting the random selection to ensure the sample included a variety of cloud service providers and DOD components. We are not disclosing the

[6]GAO, *Information Technology Reform: Progress Made but Future Cloud Computing Efforts Should be Better Planned*, GAO-12-756 (Washington, D.C.: July 11, 2012).

[7]H.R. Rep. No. 117-397, at 321 (2022), accompanying the James M. Inhofe National Defense Authorization Act for Fiscal year 2023, Pub. L. No 117-263, 136 Stat. 2395 (2022). For the purposes of this report, restrictive software licensing practices include any enterprise agreements or vendor processes that limit, impede, or prevent DOD efforts to use software in cloud or multi-cloud computing.

[8]According to DOD Directive 8000.01, an IT investment is the expenditure of IT resources to address mission delivery and management support. An IT investment may include a project or projects for the development, modernization, enhancement, or maintenance of a single IT asset or a group of IT assets with related functionality, and the subsequent operation of those assets in a production environment.

[9]The SNaP-IT system is a database application used to collect and assemble information required in support of the IT budget request submitted to Congress.

names of the investments or cloud service providers in this report due to the sensitivity of the information.[10]

To assess the reliability of the SNaP-IT data, we reviewed documentation related to the system (e.g., data dictionary) and reviewed the data for obvious issues, including missing or questionable values. We also interviewed officials in charge of SNaP-IT data within the DOD Office of the Chief Information Officer (CIO) regarding department's guidance for using the system and about how the department ensures the quality and reliability of the data. We found that the data were sufficiently reliable for our purpose of selecting investments for a more detailed review.

To address our first objective, we first identified a non-generalizable sample of DOD component agencies (components) based on the size of their cloud budgets for fiscal year 2023. We selected three components with the largest cloud budget requests—the Army, Air Force, and Navy—to interview. Specifically, we interviewed officials from each component's cloud computing office. The structured interviews focused on the impacts of restrictive enterprise software licensing practices on the selected components' investments, their practices for mitigating the impacts, and relevant documentation of impacts or mitigation activities.

We also performed structured interviews of the selected investments' IT project and acquisition management staffs about any impacts the investments had encountered from restrictive software licensing practices. We combined the data from the structured interviews from all entities (selected components and investments) and analyzed and summarized the results.

To address our second objective, we reviewed ISACA's Capability Maturity Model Integration v2.2 and selected relevant practices in the areas of acquisition and risk management.[11] We selected these areas because they aligned closely with cloud computing, commercial software licensing, and acquisition. We organized the selected practices into two

[10]The selected investments represent six different DOD components (the Army, Air Force, Defense Human Resources Activity, Defense Information Systems Agency, Defense Logistics Agency, and Navy (not including the Marine Corps)) and four different cloud service providers. Our work focused on DOD and thus, we did not provide vendors with an opportunity to respond to these examples. The names of certain selected investments also incorporated the names of cloud service providers.

[11]ISACA, *CMMI Model V2.2* (Pittsburgh, PA: Mar. 10, 2021). CMMI Model and ISACA ©[2021] All rights reserved. Used with permission.

key activities: (1) identifying and analyzing impacts of restrictive practices during the acquisition process and for established IT investments or projects, and (2) developing plans for mitigating adverse impacts. We then compared the investments' efforts to mitigate the potential impact of restrictive software licensing practices to these practices.

Specifically, we asked the selected investment teams and their portfolio managers to provide documentation describing their efforts to mitigate the potential impact of restrictive software licensing practices (e.g., acquisition documentation, risk management plans, and mitigation plans) and address the identified key practices. Additionally, we interviewed relevant officials from the investments to identify any gaps in the documentation. We compared the investments' efforts to the selected evaluation criteria to determine whether they had implemented the practices.

We also obtained relevant DOD plans (e.g., *the DOD Cloud Computing Strategy*[12] and DOD Software Modernization Implementation Plan[13]) and guidance (e.g., DOD's *Requirements for the Acquisition of Digital Capabilities Guidebook)* and analyzed any content related to restrictive software licensing practices. In addition, we interviewed officials from the DOD's Office of CIO and Enterprise Software Initiative (ESI) regarding their experience with impacts of restrictive practices through their support of cloud computing efforts throughout the department. We also discussed with them the department's plans and guidance on restrictive enterprise software licensing practices and mitigation strategies. Further details on our objectives, scope, and methodology are provided in appendix I.

We conducted this performance audit from October 2022 to September 2023 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.

[12]Department of Defense, *DOD Cloud Strategy* (Dec. 2018).

[13]Department of Defense, *Software Modernization Implementation Plan* (Washington, D.C.: March 30, 2023).

Background

Purchasing IT services through a cloud service provider enables agencies to avoid paying for all the computing resources that would typically be needed to provide such services. This approach offers federal agencies a means to buy services more quickly and possibly at a lower cost than building, operating, and maintaining these computing resources themselves.

Commercial software typically includes initial license fees and additional fees for continued use of the software. These fees may include, as part of the license agreement, access to product support and/or other services, including upgrades.[14] Licensing models and definitions may significantly differ depending on the software product and vendor.

In December 2010, OMB made cloud computing an integral part of its *25 Point Implementation Plan to Reform Federal Information Technology Management*.[15] The plan called for the development of a government-wide strategy to hasten the adoption of cloud services. To accelerate the shift, OMB required agencies, including DOD, to identify three systems to migrate to cloud services, create a project plan for migration, and migrate all three systems by June 2012.

Subsequently, in February 2011, OMB issued the *Federal Cloud Computing Strategy*, that required each agency's CIO to evaluate safe, secure cloud computing options before making any new investments.[16] The strategy provided definitions of cloud services; benefits of cloud services, such as accelerating data center consolidations; a decision framework for migrating services to a cloud environment;[17] case studies

[14]GAO, *Federal Software Licenses: Better Management Needed to Achieve Significant Savings Government-Wide*, GAO-14-413 (Washington, D.C.: May 22, 2014).

[15]Office of Management and Budget, *25 Point Implementation Plan to Reform Federal Information Technology Management* (Washington, D.C.: Dec. 9, 2010).

[16]Office of Management and Budget, *Federal Cloud Computing Strategy* (Feb. 8, 2011).

[17]The decision framework, among other things, identified several key areas for determining the readiness for moving to a cloud environment, including the ability of the cloud service provider to address government security requirements.

to support agencies' migration to cloud services; and roles and responsibilities for federal agencies.

According to the National Institute of Standards and Technology (NIST),[18] cloud computing offers federal agencies a number of benefits:

- **On-demand self-service.** Agencies can, as needed, provision computing capabilities, such as server time and network storage, from the service provider automatically and without human interaction.
- **Broad network access.** Agencies can access needed capabilities over the network through workstations, laptops, or other mobile devices.
- **Resource pooling.** Agencies can use pooled resources from the cloud provider, including storage, processing, memory, and network bandwidth.
- **Rapid elasticity. Agencies** can provision the resources that are allocated to match what actual resources are needed according to demand. This is done by scaling resources up or down by adding or removing processing or memory capacity, or both, according to demand.
- **Measured service.** Agencies can pay for services based on usage. This allows agencies to monitor, control, and generate reports, providing greater transparency into the agency's use of cloud services.

As noted in NIST guidance, cloud service providers have established three types of service models that are offered to consumers:

- **Infrastructure as a service.** The service provider delivers and manages the basic computing infrastructure of servers, software, storage, and network equipment. The consumer provides the operating system, programming tools and services, and applications.
- **Platform as a service.** The service provider delivers and manages the infrastructure, operating system, and programming tools and services, which the consumer can use to create applications.
- **Software as a service.** The service provider delivers one or more applications and all the resources (operating system and

[18]National Institute of Standards and Technology, *The NIST Definition of Cloud Computing*, Special Publication 800-145 (Gaithersburg, MD: Sept. 2011).

programming tools) and underlying infrastructure to run them for use on demand.

In June 2019, OMB issued an update to its *Federal Cloud Computing Strategy* in an effort to accelerate agency adoption of cloud-based solutions.[19] The strategy focused on equipping agencies with the tools needed to make informed IT decisions according to their mission needs. In addition, the strategy included 14 key requirements for agencies to implement within three areas—security, procurement, and workforce—that were intended to help ensure successful cloud implementation.

DOD Cloud Computing and Software License Management Roles and Responsibilities

DOD spends billions of dollars each year on IT systems that are fundamental to achieving its mission. In fiscal year 2023, the department plans to spend approximately $45.1 billion on unclassified IT investments. Over the past decade, DOD has worked on multiple efforts to advance cloud computing in accordance with the laws, department policies, and strategies that assigned roles and responsibilities for cloud and commercial software license management throughout the department. DOD's CIO is ultimately responsible for the department's information enterprise, including eliminating duplicative IT within and between components and identifying opportunities for IT efficiencies.[20]

However, federal statute and DOD policy have assigned IT responsibilities to other, non-CIO stakeholders as well.[21] For example, the Office of the Under Secretary of Defense for Acquisition and Sustainment is responsible for developing policies for the acquisition and development of new IT systems. As a result, the CIO coordinates with stakeholders in various committees using collaborative mechanisms, such as a working group, when implementing significant cloud or rationalization efforts.

[19]Office of Management and Budget, *Federal Cloud Computing Strategy* (Washington, D.C.: June 24, 2019).

[20]Department of Defense, *Department of Defense Chief Information Officer*, Department of Defense Directive 5144.02, (Sept. 19, 2017).

[21]*See, e.g.,* 10 U.S.C. § 4571 note (2019) (Authority for Continuous Integration and Delivery of Software Applications and Upgrades to Embedded Systems).

In addition, each of the selected DOD components has established cloud offices responsible for component services. This includes providing access to an enterprise cloud, facilitating cloud migrations, and offering common shared services to mission owners.[22]

Regarding managing its software licenses, DOD's Enterprise Software Initiative (ESI) is responsible for leading the establishment and management of enterprise commercial-off-the-shelf software IT agreements, assets, and policies. ESI's leadership of these efforts is for the purpose of lowering total cost of ownership across DOD, Coast Guard, and Intelligence Communities. ESI's mission extends across the entire commercial IT life cycle and is intended to leverage DOD's combined buying power with commercial software publishers, hardware vendors, and service providers.

ESI establishes and offers standard terms and costs for enterprise software agreements and promotes their use.[23] ESI offers different categories of enterprise agreements, including those focused on software, IT asset management,[24] cybersecurity, IT services, and hardware.

According to ESI's website, ESI and DOD components supported 106 enterprise agreements as of May 2023.[25] Of the agreements, 91 were designed to deliver software, including software for IT asset management, cybersecurity, engineering and computer-aided design, modeling and simulation, software-as-a-service, and professional services. Of the enterprise agreements focused on cloud computing, 18 provided software for cloud computing and one agreement provided cloud services.

ESI also provides department-wide guidance about planning for and establishing software license agreements, including a software buyer's

[22]The cloud offices for the selected components included the Air Force Cloud One service and platform, Army's Enterprise Cloud Management Agency, and the Navy Program Executive Office for Digital and Enterprise Services, which provides technical services and expertise to support the Navy Digital Platform and cloud computing.

[23]ESI does not dictate the products or services to be acquired through its agreements.

[24]According to ESI, IT asset management is the set of business practices that join financial, contractual, and inventory functions to support strategic decision making and life cycle management for the IT environment.

[25]https://www.esi.mil/AgreementList.aspx?type=0.

checklist and a software license risk assessment tool. The tools provide questions components and investment teams can use to plan their acquisitions. The tools also point to additional relevant DOD guidance.

DOD Plans and Guidance about Cloud Computing and Managing Software

In July 2012, DOD's CIO issued the *DOD Cloud Computing Strategy,* which aligned the department with federal requirements[26] to consider cloud options before making new IT investments.[27] The department's strategy noted that the CIO was committed to providing a secure, resilient enterprise cloud environment through an alignment with department-wide IT efficiency initiatives, federal data center consolidation, and cloud computing efforts. The strategy also identified steps necessary for the department's transition to an enterprise-wide cloud environment.

Additionally, in December 2018, the cloud strategy was updated to align with the department's implementation of an enterprise cloud environment.[28] DOD acknowledged that it lacked clear guidance on cloud computing, adoption, and migration and that it had stood up a number of cloud efforts that had not been designed for enterprise use. According to the strategy, the interoperability of the multi-vendor and multi-cloud environment was intended to be governed by one overarching enterprise cloud strategy.

One of the strategy's guiding principles was to leverage industry open standards and best practices to avoid vendor lock-in and provide maximum flexibility for future cloud advances. The strategy noted that the DOD CIO planned to organize forums to bring together all lessons learned and find ways to integrate these lessons into DOD policies, procedures, and acquisition strategies moving forward.

DOD has specific acquisition regulations and policies that govern the procurement of commercial software and software that is developed either wholly or partially at government expense (non-commercial

[26]Office of Management and Budget, *25 Point Implementation Plan to Reform Federal Information Technology Management*.

[27]Department of Defense, *DOD Cloud Computing Strategy* (July 2012).

[28]Department of Defense, *DOD Cloud Strategy* (December 2018).

software). These policies and procedures address the government's rights in what is developed.[29] In January 2020, DOD reissued and updated its acquisition policies, emphasizing speed and agility in the acquisition process.[30] The updated instruction established the *Adaptive Acquisition Framework,* comprised of six acquisition pathways. These six acquisition pathways are intended to, among other things, deliver solutions to the end user in a timely manner.

One of the pathways, the software acquisition pathway, is intended to promote the timely acquisition of commercial software and custom software capabilities developed for DOD, either partially or wholly funded by the government. Specifically, this pathway notes that the department prefers to leverage existing enterprise services over creating unique software services for individual programs.[31] According to the policy, program managers are to understand the rights of government and industry, as well as the system and software architecture and lifecycle requirements. The policy calls for managers to use this knowledge to make decisions regarding procuring commercial software and negotiate for computer software deliverables and license rights under government development contracts for software that is developed either partially or wholly at government expense.

[29]The government obtains technical data and license rights to software in accordance with the Federal Acquisition Regulation (FAR), agency supplements to the FAR, and any specifically negotiated licenses in the contract. These rights control how the government can use, disclose, or reproduce contractor owned information in which the government has expended funds. Department of Defense, *Defense Federal Acquisition Regulation Supplement*, Subparts 227.7103 and 227.7203 (Revised September 23, 2016). The rights detailed in these sections do not apply to commercial software that is procured by the government in which the government has not expended funds to develop, and is only obtaining a license to use the software. See generally, FAR 12.212 (Computer software) and *Defense Federal Acquisition Regulation Supplement* 227.7202-3 (Rights in commercial computer software or commercial computer software documentation). For commercial software, the government obtains only those rights specified in the license under which the commercial computer software or commercial computer software documentation was obtained. *Defense Federal Acquisition Regulation Supplement* 227.7202-3(a).

[30]Department of Defense, Department of Defense Directive 5000.01, *The Defense Acquisition System* (Sept. 9, 2020) and Department of Defense Instruction 5000.02, *Operation of the Adaptive Acquisition Framework* (Change 1, June 8, 2022).

[31]Department of Defense, Department of Defense Instruction 5000.87, *Operation of the Software Acquisition Pathway* (Oct. 2, 2020).

In February 2022, the department published *its Department of Defense Software Modernization Strategy,*[32] which replaced its 2018 cloud strategy. One of the key goals was to accelerate the DOD enterprise cloud environment as the foundation for software modernization using a multi-cloud, multi-vendor approach.

Also in February 2022, DOD's CIO issued additional acquisition guidance governing digital capabilities acquired through the DOD Adaptive Acquisition Framework.[33] The guidebook identified the need to consider cost in licensing, noting its potentially significant impact. The guidebook described different licensing models that might increase costs and includes a specific section governing the unique requirements in acquiring cloud services. The guidebook states that program managers should consider all acquisition approaches, consider contract types and flexibilities, and ensure that all cloud licensing fees are known.

In March 2023, the department issued the *DOD Software Modernization Implementation Plan*.[34] The plan includes tasks for increasing the adoption of enterprise-approved clouds, increasing agility in acquisition implementation, and promoting software modernization across all acquisition pathways. It also states that task execution and software modernization success will rely heavily on DOD components that are performing the work associated with planning and product development as part of existing programs.

Further, the plan notes that software modernization is not a standalone effort—it does not have its own budget, dedicated resources, or program of record. Instead, it is an integral part of every mission.

[32]Department of Defense, *Department of Defense Software Modernization Strategy* (Washington, D.C.: Feb. 2, 2022). The Software Modernization Senior Steering Group leads the implementation of the software modernization activities supporting the strategy. This group is chaired by the DOD Deputy CIO for Information Enterprise, a senior representative from the Office of the Under Secretary of Defense for Acquisition and Sustainment, and a senior representative from the Office of the Under Secretary of Defense for Research and Engineering.

[33]Department of Defense Chief Information Officer, *Requirements for the Acquisition of Digital Capabilities Guidebook* (February 2022).

[34]Department of Defense, *Software Modernization Implementation Plan* (Washington, D.C.: March 30, 2023).

GAO Has Previously Reported on Software License Management and DOD Cloud Computing

In May 2014, we found that DOD—like many other agencies—did not have a fully centralized approach for managing commercial software licenses, establish a comprehensive inventory for tracking and maintaining these licenses, regularly track and maintain an inventory with tools and metrics, or provide sufficient training on software management.[35] For example, DOD partially met best practices for its software license management policy; however, it lacked provisions for centralized management, tracking inventory, and lifecycle software license management. Further, the department had not analyzed its software license data to inform investment decisions.

In October 2017, DOD implemented the six recommendations by establishing a central software license management approach, creating a software license inventory, and analyzing software license data, among other actions.

In June 2022, we found that DOD had taken steps to address OMB's key cloud requirements related to securing its cloud environments and improving the procurement of these services over the past decade. However, the department had not initiated an effort to ensure it had the current and future workforce it needed to support its planned enterprise-wide cloud environment.[36] Furthermore, we reported DOD lacked time frames and a long-term plan for application rationalization.[37] We also identified issues with completeness of the department's cloud spending data, based on Technology Business Management framework cost categories, which increased the likelihood that cloud spending data was underreported.

[35]GAO, *Federal Software Licenses: Better Management Needed to Achieve Significant Savings Government-Wide*, GAO-14-413 (Washington, D.C.: May 22, 2014).

[36]GAO, *Cloud Computing: DOD Needs to Improve Workforce Planning and Software Application Modernization*, GAO-22-104070 (Washington, D.C.: June 29, 2022).

[37]OMB published its Federal Cloud Computing Strategy in June 2019, called Cloud Smart. This required all federal agencies to rationalize their application portfolios—streamlining the portfolio with the goal of improving efficiency, reducing complexity and redundancy, and lowering the cost of ownership.

We made nine recommendations to DOD related to addressing gaps in cloud workforce activities, improving application rationalization planning, and updating guidance on Technology Business Management framework implementation. DOD agreed with one recommendation, partially agreed with seven, and did not agree with one. All nine recommendations had not yet been implemented as of July 2023.

In April 2023, we reported[38] that DOD had partially implemented most of the recommendations to improve DOD's software practices issued by two Federal Advisory Committees[39]—the Defense Science Board[40] and Defense Innovation Board.[41] However, the department had not fully implemented key practices to facilitate future software modernization plans. In addition, DOD had not yet fully developed an approach to hold accountable the many leaders who needed to be involved in implementing software modernization reforms.

[38]GAO, *Software Acquisition: Additional Actions Needed to Help DOD Implement Future Modernization Efforts*, GAO-23-105611 (Washington, D.C.: Apr. 5, 2023).

[39]The two committees were established pursuant to the Federal Advisory Committee Act, Pub. L. No. 92-463, 86 Stat.770 (1972) (codified at 5 U.S.C. §§ 1001-14). We have previously reported that advisory committees play an important role in informing public policy and government regulations by advising the President and federal agencies on national issues. These committees perform peer reviews of scientific research, develop recommendations on specific policy decisions, identify long-range issues facing the nation, and evaluate grant applications. The committees' advice can enhance the quality and credibility of federal decision-making. GAO, *Federal Advisory Committees: Actions Needed to Enhance Decision-Making Transparency and Cost Data Accuracy*, GAO-20-575 (Washington, D.C.: Sept. 10, 2020).

[40]The Defense Science Board serves as the Federal Advisory Committee chartered to provide DOD leadership with independent advice and recommendations on science, technology, and acquisition processes, among other things. In January 2013, the board's Task Force on Cyber Security and Reliability in a Digital Cloud issued a report with recommendations focused on improving implementation of cloud computing, among others.

[41]The Defense Innovation Board serves as the Federal Advisory Committee chartered to provide DOD leadership with independent recommendations to DOD leaders on emerging technologies and innovative approaches. In 2019, the board recommended that DOD adopt industry standards for cloud computing and modernize its computing environment for application developers and end users, among other things.

Selected DOD Entities Reported Various Impacts of Restrictive Software Licensing Practices

All three selected DOD components and two of the six selected investments reported that restrictive software license practices impacted their cloud computing efforts. The selected DOD components and investments identified specific restrictive software licensing practices the department has encountered. Specifically, they noted that vendors

- limited the ability to migrate the department's software obtained through pre-existing, traditional commercial software licenses to cloud computing;
- established terms and conditions that limited DOD access to previous versions of software;[42]
- established terms and conditions that impeded the department's use of specific software by requiring compatibility with specific versions of software from other vendors;
- limited software available for cloud computing in certain commercial markets where the vendor had significant market share;
- restricted DOD's use of software to the vendor's proprietary cloud or a limited number of competitor cloud solutions;
- prevented DOD from operating software on specific cloud platforms; and[43]
- sold software that met DOD requirements only in packages with other software not needed to meet requirements.

Officials from the selected components and investments stated that restrictive practices generally impacted the (1) cost of cloud computing, (2) choice of cloud service providers, and (3) other related impacts. Table

[42]The investments reporting this restrictive practice had obtained commercial software from vendors that required compatibility with prior versions of a different vendor's software. However, the vendor of that software limited use of prior versions to investments using its own cloud service. The investments in question relied on different cloud service providers and were unable to access the previous versions under the established enterprise agreement.

[43]The investments reporting this restrictive practice encountered it because they were trying to use commercial software on a different cloud service provider than the one authorized by the software vendor.

1 describes impacts of restrictive software licensing practices encountered by the selected DOD components and investments.

Table 1: Impacts of Restrictive Software Licensing Practices Encountered by Selected Department of Defense (DOD) Components and Investments

Impact type	Impact description
Cost of cloud computing	• Infrastructure costs increased because two vendors required additional fees to use their software with third party cloud service providers. Officials were unable to specify the actual amount of increase.
	• Licensing costs increased because one vendor bundled frequently used software with other software, making it available only at the bundled price.[a] Officials were unable to specify the actual amount of increase.
	• Licensing costs for migrating one vendor's software to the cloud increased because the vendor required repurchase of same licenses for use in cloud. Officials were unable to specify the actual amount of increase.
	• Total investment life cycle cost increased dramatically because one vendor had offered original software licenses at a discounted or low price, but increased the cost of adding additional licenses significantly. Adding licenses later in the selected investment cost more than the original purchase price.[b] Officials were unable to specify the actual amount of increase.
	• Costs for migrating one vendor's software to the cloud under existing licenses increased. Officials estimated that costs increased, but were unable to specify the amount.
Choice of cloud provider	• One component establishing a cloud platform for component-wide use opted to avoid using one cloud service provider from whom it had previously purchased on-premise software licenses because of that vendor's restrictive licensing practices.
	• Two components were limited in the cloud service providers they could use because one vendor limited its software's use to only selected commercial partners' cloud service providers or its own cloud.
	• One investment's selected software solution required DOD to deploy the software on a specified cloud service provider's infrastructure.
	• One investment team that had not yet encountered impacts from restrictive practices noted that implementing the investment and its architecture for such a large investment had effectively created vendor lock-in. Vendor lock-in may occur without explicitly documented restrictive terms and conditions. They explained that changing from the current configuration to a different cloud service provider would be cost prohibitive.[c]
Other	• Officials from one component noted that two software vendors required interoperability with a previous version of a different vendor's software and that conflicts exist among specific software vendor requirements. However, the different vendor does not allow customers to use the previous version unless they are using that vendor's cloud service platform.[d]
	• One component intends to adopt a proprietary software for the cloud. However, it faces the risk that the software vendor will not help sustain the product because the component is not using the specified cloud service provider.

Source: GAO analysis of data from selected DOD components and investments. | GAO-23-106290

[a]DOD cybersecurity requirements increased licensing costs for one vendor's access control software because the department needed to purchase multiple licenses for the subset of end users who also required higher-level privileges.

[b]In another case, restrictive practices designed to increase costs were not in place, but one selected component's underestimation of license needs for a software development platform led to implementation delays and delayed use of the platform by additional customers.

[c]Two of the impacts listed in this table were reported by a component managing one of the selected investments. We included the impacts reported by this additional component in our table.

[d]The component reporting this impact may also face substantial impact on costs associated with the proposed solution. If the component purchases licenses through another existing DOD agreement, the unit cost for the licenses would increase from $.19 per unit to more than $385 per unit.

Officials managing four of the six selected investments did not identify impacts on their investments from restrictive software licensing practices. The officials explained that most of these investments were configured to support deployment of software within the cloud. In such cases, officials stated that the investments' designs originally establishing the software in the cloud—rather than migrating existing licenses to the cloud—limited the likelihood that it would encounter restrictive practices.

DOD Had Gaps in Guidance and Plans for Mitigating Impacts of Restrictive Software Licensing Practices

Effectively managing software licenses for cloud computing involves, among other things, applying industry best practices for acquisition and risk management.[44] Key activities for mitigating impacts of restrictive software licensing practices for cloud computing include (1) identifying and analyzing impacts of restrictive practices during the acquisition process and for established IT investments or projects and (2) developing plans for mitigating adverse impacts.

DOD had gaps in its guidance for mitigating the impacts of restrictive software licensing practices. DOD's guidance and plans did not specifically address analyzing impacts of restrictive practices during the acquisition process and identifying and analyzing impacts related to restrictive software licensing practices for established IT investments.[45] DOD's plans also did not require components to mitigate impacts of restrictive software licensing practices. In addition, DOD's guidance did not call for mitigation plans to address impacts of restrictive software

[44]ISACA, *CMMI Model V2.2* (Pittsburgh, PA: Mar. 10, 2021). CMMI Model and ISACA ©[2021] All rights reserved. Used with permission.

[45]Department of Defense, *Department of Defense Risk, Issue, and Opportunity Management Guide for Defense Acquisition Programs* (Jan. 2017); *Cloud Strategy; Software Modernization Strategy; Software Modernization Implementation Plan; Requirements for the Acquisition of Digital Capabilities Guidebook*; and *Operation of the Software Acquisition Pathway*.

licensing practices. Further, the six selected investments also did not fully address the key activities.

DOD Guidance and Plans Did Not Fully Address Key Activities for Mitigating Impacts of Restrictive Software Licensing Practices

DOD's policy and guidance documents addressed identifying impacts related to restrictive software licensing practices during the acquisition process. Specifically, the department has established guidance—the website for ESI[46]—that components and investments can use when selecting software suppliers to avoid or minimize any agreements that incorporate restrictive practices.[47] The following documents and tools are part of that guidance.

- DOD's *Requirements for the Acquisition of Digital Capabilities Guidebook* emphasizes the importance of planning during the acquisition process for cloud licensing models and encourages project managers to ensure that contracts include all cloud licensing fees.[48] Specifically, the guidebook asks officials to consider the scope of each license for planned systems or applications.[49]
- DOD's *System Engineering Guidebook* describes the role system engineers have in planning for software license costs.[50] The guidebook notes that one concern with using commercial software is that licensing agreements vary and can be restrictive. The guidance

[46]https://www.esi.mil. DOD regulations direct departments and agencies to fulfill requirements for commercial software and commercial software services in accordance with the DOD Enterprise Software Initiative. On its website, ESI promotes the use of enterprise software agreements with contractors that allow DOD to obtain favorable terms and pricing for commercial software. Department of Defense, *Defense Federal Acquisition Regulation Supplement* § 208.7402(a).

[47]Department of Defense, Department of Defense Instruction 5000.82 – *Requirements for the Acquisition of Digital Capabilities* and *Defense Federal Acquisition Regulation Supplement* § *208.7402* (Enterprise Software Agreements).

[48]Department of Defense Chief Information Officer, *Requirements for the Acquisition of Digital Capabilities Guidebook* (February 2022).

[49]The guidebook points out how the different cloud licensing models can have substantial impacts on cost.

[50]Department of Defense, *Department of Defense Office of the Under Secretary of Defense for Research and Engineering: Systems Engineering Guidebook* (February 2022).

also notes that using commercial software can provide significant opportunities for efficiencies but can also introduce certain issues that should be considered and mitigated if the program is to realize the expected benefits.

- ESI's master agreement template includes terms and conditions intended to avoid or minimize the likelihood that components enter into agreements with restrictive terms and conditions. For example, the master agreement template recommends language that would permit DOD to deploy licenses with any third-party cloud service provider and transfer licenses between on-premises data centers and third party cloud service providers, or between third party cloud service providers without charge, limitation, or change in functionality.
- ESI's *Software License Risk Assessment Tool* is designed to help software buyers review a seller's proposed license agreement to determine the areas of risk that should be addressed in a negotiation and to initiate and document negotiations with software vendors. For example, the tool provides a worksheet for planning for permitted uses, transfers rights, and third party software. The tool also includes a question about whether the licensing agreement includes a clearly stated basis for pricing the software license.
- A DOD ESI white paper titled, *Best Practice Clauses for Software License Grants,* provides 15 different clauses for teams to consider including in their software licensing agreements. The paper provides recommended terminology for each clause and explains the rationale for including it. For example, the paper includes a clause for granting DOD a perpetual license to use the software.
- ESI compiles a list of its existing original equipment manufacturer agreements that have specific key negotiated terms and conditions addressing DOD rights.[51] These agreements are designed to remove restrictions for components and investment teams when migrating on-premise software to the cloud. For example, in May 2023, DOD reported that about 90 percent of the ESI agreements with software publishers for on-premise license models contained language adapting the recommended ESI language granting rights to deploy and use licenses in a cloud computing environment. Similarly, DOD reported that all of the ESI agreements that included a software as a service licensing model (about 30 percent of ESI's agreements with

[51]According to Department of Defense, *Defense Federal Acquisition Regulation Supplement* 202.101, an original equipment manufacturer means a company that manufactures products that it has designed from purchased components and sells those products under the company's brand name.

more than 100 original equipment manufacturers) addressed data ownership in a cloud environment.

However, the DOD CIO and ESI have not fully developed or implemented guidance for (1) identifying and analyzing impacts of restrictive software licensing practices and (2) mitigating impacts of restrictive software licensing practices on cloud computing efforts. In particular, DOD's and ESI's guidance and plans did not specifically address analyzing impacts of restrictive practices during the acquisition process and identifying and analyzing impacts of restrictive software licensing practices for established IT investments. For example, although the department has developed a risk framework, cloud and software modernization guidance, a cloud strategy, a software modernization plan, and a software acquisition pathway,[52] none of the guidance and plans specifically discuss practices analyzing impacts of restrictive practices during the acquisition process or identifying and analyzing risks related to restrictive software licensing practices for established investments. DOD's plans also did not require components to mitigate impacts of restrictive software licensing practices. In addition, DOD's guidance did not require plans for mitigating impacts of restrictive software licensing practices.

DOD officials acknowledged that the department has not fully developed guidance and plans addressing the key activities needed for mitigating impacts of restrictive practices.

Without comprehensive guidance for mitigating the impacts of restrictive software licensing practices, the department is not well positioned to identify and analyze the impact of such practices or to mitigate any risks they present in an efficient and effective manner. Developing and implementing such guidance and plans could improve the quality and consistency of DOD's practices for identifying, analyzing, and mitigating impact of restrictive practices.

[52]Department of Defense, *Department of Defense Risk, Issue, and Opportunity Management Guide for Defense Acquisition Programs* (Jan. 2017); *Cloud Strategy; Software Modernization Strategy; Software Modernization Implementation Plan; Requirements for the Acquisition of Digital Capabilities Guidebook;* and *Operation of the Software Acquisition Pathway.*

Selected Investments Did Not Consistently Address Key Activities for Mitigating Impacts of Restrictive Software License Practices

The six selected investments did not consistently address the key activities for (1) identifying and analyzing impacts of restrictive software licensing practices during the acquisition process and for established IT investments and (2) developing plans for mitigating adverse impacts. Two investments partially addressed the key activities. Four other investments did not address the key activities. Specifically,

- For the first selected investment, the team addressed the first key activity during the acquisition process by identifying a risk related to vendor terms and conditions limiting DOD access to previous versions of software. In addition, officials managing that investment described ad hoc activities they performed to analyze the identified risk related to vendor terms and conditions limiting DOD access to previous versions of software. For example, the investment team consulted with DOD ESI and ultimately found a different agreement to meet its requirements.[53]

  However, the investment team did not address the second key activity. Although officials reported that they may, in the future, develop risk mitigation plans to manage the identified impacts and mitigation strategies, they have not yet done so.

- For the second investment, the team also partially addressed the key activities. For example, the selected investment identified the impact of a restrictive practice for the established investment affecting part of the cloud infrastructure. The vendor's virtualization software incorporated in the investment through the established agreements had not been designed for use in cloud computing and began creating challenges for managing investment cloud resources. The investment team was not able to find a viable replacement for the software, so it informed the vendor of the issue and requested that it be resolved.

  However, the investment did not fully assess the impact of this restrictive practice. Specifically, the investment team did not perform a risk assessment or other formal analysis. Also, the team did not

[53]According to investment officials, addressing this impact took more than 8 months.

develop risk mitigation plans or other formal plans for managing the impact.

- The third selected investment did not address the key activities. The investment team reported that it designed a cloud solution to be cloud agnostic and avoid restrictive software licensing practices impacting its choice of providers. The team reported that they did not encounter restrictive practices and therefore did not need to mitigate any impacts.
- The fourth selected investment did not address either key activity for mitigating restrictive practices. For that investment, cost was the overriding factor in selection of software for cloud computing. As a result, the team did not work to avoid or minimize impacts of restrictive software licensing practices during the acquisition process or address the other key activity.
- The fifth and sixth selected investments also did not address either key activity for mitigating restrictive practices. The investment teams did not perform any assessment of potential impacts of restrictive practices during the acquisition process or for established investments. The investments did not identify restrictions. Lacking guidance to identify and analyze impacts during the ongoing investments, they did not address the second key activity.

Officials responsible for all six selected investments stated they were unaware of any available DOD guidance regarding restrictive software licensing practices. They added that DOD's guidance did not specifically instruct investments to mitigate impacts of restrictive software licensing practices and its processes did not explicitly require any assessment of restrictive practices for established investments. Of the five selected investments that did not identify any impacts during the acquisition process, four did not take additional action to identify, analyze, or mitigate impacts of restrictive practices.

Until DOD updates and implements guidance and plans for mitigating the impacts of restrictive software licensing practices, the selected investments will continue to implement inconsistent, ad hoc approaches that can be ineffective at identifying and mitigating the department's risks. In addition, the full extent of impacts from restrictive software licenses on the department remains unknown.

Conclusions

Restrictive software licensing practices adversely impacted DOD cloud computing efforts. The restrictive practices generally impacted the cost or choice of provider. Certain types of investments, such as those migrating existing software to cloud computing, were more likely to encounter restrictive practices.

DOD had gaps in its guidance and plans for mitigating impacts of restrictive software licensing practices. ESI had developed guidance and plans designed to aid in identifying impacts associated with restrictive practices during the acquisition process. However, none of the department's guidance or plans specifically addressed analyzing impacts of restrictive practices during the acquisition process, identifying and analyzing restrictive software licensing practices for established IT investments, or mitigating impacts of restrictive practices. Moreover, the selected investments did not consistently address the key activities for mitigating restrictive software licensing risks. Until DOD updates and implements guidance and plans for mitigating the impacts of restrictive software licensing practices, the selected investments will continue to implement ad hoc approaches likely to be ineffective at identifying and mitigating such impacts.

Recommendation for Executive Action

We are making one recommendation to DOD:

The Secretary of Defense should direct the DOD CIO, in coordination with ESI, to update and implement guidance and plans to fully address identifying, analyzing, and mitigating the impacts of restrictive software licensing practices on cloud computing efforts. (Recommendation 1)

Agency Comments

We provided a draft of this report to DOD for review and comment. In its comments reproduced in appendix II, DOD concurred with the recommendation and described plans and time frames for completing actions intended to address the recommendation. Specifically, DOD stated that it intends to issue guidance to, among other things, close the gaps identified in this report, further streamline and enhance the

procurement process, and expand collaboration among stakeholders. In addition, DOD plans to provide a clear definition of restrictive software license practices and their potential risk on cloud computing efforts. The DOD CIO intends to publish this updated guidance by the end of fiscal year 2024.

We are sending copies of this report to the appropriate congressional committees and the 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 members have any questions on matters discussed in this report, please contact me at (202) 512-4456 or Harriscc@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 III.

Carol C. Harris
Director, Information Technology, Management Issues

List of Committees

The Honorable Jack Reed
Chairman
The Honorable Roger Wicker
Ranking Member
Committee on Armed Services
United States Senate

The Honorable Jon Tester
Chair
The Honorable Susan Collins
Ranking Member
Subcommittee on Defense
Committee on Appropriations
United States Senate

The Honorable Mike Rogers
Chairman
The Honorable Adam Smith
Ranking Member
Committee on Armed Services
House of Representatives

The Honorable Ken Calvert
Chair
The Honorable Betty McCollum
Ranking Member
Subcommittee on Defense
Committee on Appropriations
House of Representatives

Appendix I: Objectives, Scope, and Methodology

House Report 117-397 accompanying the James M. Inhofe National Defense Authorization Act for Fiscal Year 2023 included provisions for GAO to review the impact that restrictive software licensing practices could have on the Department of Defense (DOD) as it transitions to cloud services and leverages innovation across multiple cloud service providers.[1] The objectives for this engagement were to (1) describe how restrictive enterprise software licensing practices impact DOD cloud computing services and (2) evaluate the extent to which DOD is mitigating the potential impact of restrictive software licensing practices.

For both objectives, we also selected six DOD cloud IT investments from the department's Select and Native Programming–Information Technology (SNaP-IT) database.[2] From that database, we sorted the investments based on fiscal year 2023 budget size and removed any investment line item under $1,000,000. We then sorted the remaining investment line items into three categories—greater than $100 million, between $100 million and $10 million, and between $10 million and $1 million. We randomly selected one investment with a line item from each category to ensure our selection included one large, one medium, and one small investment. From the remaining investment line items, we selected the three investments randomly and adjusted that random selection to ensure the selected investments represented a variety of components and cloud service providers.[3] We are not disclosing the

[1]H.R. Rep. No. 117-397, at 321 (2022), accompanying the James M. Inhofe National Defense Authorization Act for Fiscal Year 2023, Pub. L. No. 117-263, 136 Stat. 2395 (2022).

[2]The SNaP-IT system is a database application used to collect and assemble information required in support of the IT budget request submitted to Congress.

[3]The six selected investments represented six different DOD components (the Army, Air Force, Defense Human Resources Activity, Defense Information Systems Agency, Defense Logistics Agency, and Navy (not including the Marine Corps)) and four different cloud service providers.

names of the investments or cloud service providers in this report due to the sensitivity of the information.[4]

To assess the reliability of the SNaP-IT data, we reviewed documentation related to the system (e.g., data dictionary) and reviewed the data for obvious issues, including missing or questionable values. We also interviewed officials in charge of SNaP-IT data within the DOD Office of the Chief Information Officer (CIO) regarding the department's guidance, the system, and how the department ensures the quality and reliability of the data. We found that the data were sufficiently reliable for our purpose of selecting investments for a more detailed review.

To address our first objective, we first identified a non-generalizable sample of DOD component agencies (components) based on the size of their cloud budgets for fiscal year 2023.[5] Specifically, we analyzed fiscal year 2023 budget request data to rank the components from the largest to the smallest cloud budget request.

We then selected three components with the largest cloud budget requests, the Army, Air Force, and Navy, to interview. Specifically, we interviewed officials from the Air Force Cloud One program, Army's Enterprise Cloud Management Agency, and the Navy Program Executive Office for Digital and Enterprise Services. The structured component interviews focused on the impacts of restrictive enterprise software licensing practices on the selected components' investments, their practices for mitigating the impacts, and relevant documentation of impacts or mitigation activities.

We also performed structured interviews of the selected investments' IT project and acquisition management staffs about any impacts the investments had encountered from restrictive software licensing practices. We also obtained supplemental written responses from the portfolio managers for the selected investments. We then combined the

[4]Our work focused on DOD and thus, we did not provide vendors with an opportunity to respond to these examples. The names of certain selected investments also incorporated the names of cloud service providers.

[5]Department of Defense, *Department of Defense Information Technology and Cyberspace Activities Budget Overview, Fiscal Year 2023, Budget Request* (Washington, D.C.: May 2022).

data from all three sets of structured interviews and analyzed and summarized the results.

To address our second objective, we reviewed ISACA's Capability Maturity Model Integration v2.2[6] and selected relevant practices in the areas of acquisition and risk management.[7] We selected these areas because they aligned with closely with cloud computing software licensing and acquisition. We then compared the investments' efforts to mitigate the potential impact of restrictive software licensing practices to these practices.

Specifically, we asked officials from the selected investments and the portfolio managers for those investments to provide documentation describing the investments' efforts to mitigate the potential impact of restrictive software licensing practices (e.g., acquisition documentation, risk management plans, and mitigation plans) and address the identified key practices. Additionally, we interviewed relevant officials from the investments to identify any gaps in the documentation. We compared the investments' efforts to the selected evaluation criteria to determine whether they had implemented the practices.

We also obtained relevant DOD plans (e.g., the *DOD Cloud Computing Strategy,*[8] *Department of Defense Software Modernization Strategy*,[9] and *DOD Software Modernization Implementation Plan*[10]) and guidance (e.g., DOD's *Requirements for the Acquisition of Digital Capabilities*

[6]ISACA, *CMMI Model V2.2* (Pittsburgh, PA: Mar. 10, 2021). CMMI Model and ISACA ©[2021] All rights reserved. Used with permission.

[7]In summarizing our two key activities as criteria for mitigating impacts of restrictive software licensing practices for cloud computing, we incorporated several specific practices from other CMMI practice areas. For example, we included specific practices from supplier source selection, supplier agreement management, and service delivery management within the acquisition process key practice. Similarly, we incorporated several practices from causal analysis and resolution into the risk management key practice.

[8]Department of Defense, *DOD Cloud Strategy* (Dec. 2018).

[9]Department of Defense, *Department of Defense Software Modernization Strategy* (Washington, D.C.: Feb. 2, 2022).

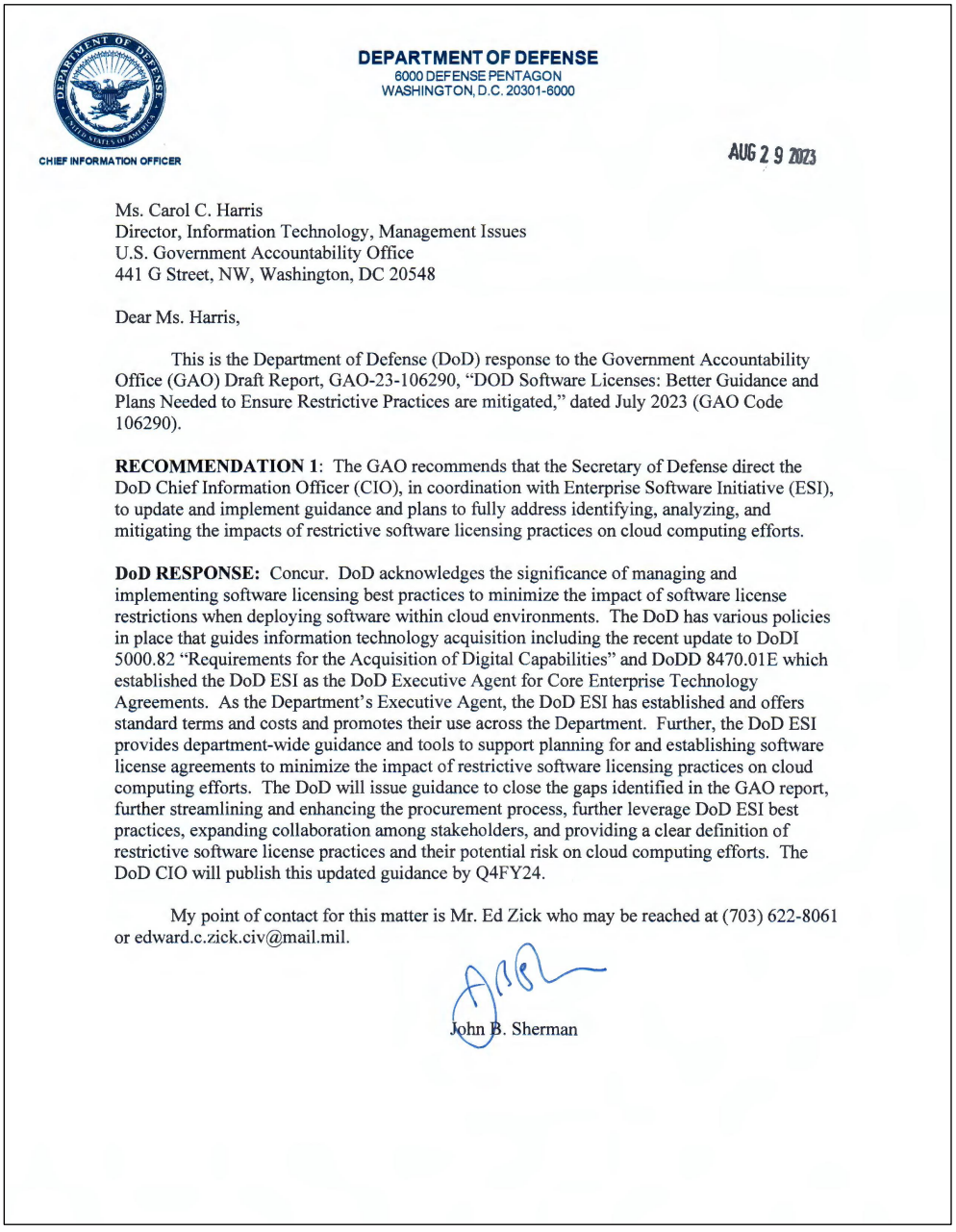
[10]Department of Defense, *Software Modernization Implementation Plan* (Washington, D.C.: March 30, 2023).

Guidebook[11] and the Enterprise Software Initiative's (ESI) Software License Risk Assessment Tool), and analyzed any content related to restrictive software licensing practices. In addition, we interviewed officials from the DOD's Office of CIO and ESI regarding their experience with impacts of restrictive practices through their support of cloud computing efforts throughout the department. We also discussed with them the department's plans and guidance on restrictive enterprise software licensing practices and mitigation strategies.

We conducted this performance audit from October 2022 to September 2023 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.

[11]Department of Defense Chief Information Officer, *Requirements for the Acquisition of Digital Capabilities* Guidebook (February 2022).

Appendix II: Comments from the Department of Defense



DEPARTMENT OF DEFENSE
6000 DEFENSE PENTAGON
WASHINGTON, D.C. 20301-6000

CHIEF INFORMATION OFFICER

AUG 2 9 2023

Ms. Carol C. Harris
Director, Information Technology, Management Issues
U.S. Government Accountability Office
441 G Street, NW, Washington, DC 20548

Dear Ms. Harris,

This is the Department of Defense (DoD) response to the Government Accountability Office (GAO) Draft Report, GAO-23-106290, "DOD Software Licenses: Better Guidance and Plans Needed to Ensure Restrictive Practices are mitigated," dated July 2023 (GAO Code 106290).

RECOMMENDATION 1: The GAO recommends that the Secretary of Defense direct the DoD Chief Information Officer (CIO), in coordination with Enterprise Software Initiative (ESI), to update and implement guidance and plans to fully address identifying, analyzing, and mitigating the impacts of restrictive software licensing practices on cloud computing efforts.

DoD RESPONSE: Concur. DoD acknowledges the significance of managing and implementing software licensing best practices to minimize the impact of software license restrictions when deploying software within cloud environments. The DoD has various policies in place that guides information technology acquisition including the recent update to DoDI 5000.82 "Requirements for the Acquisition of Digital Capabilities" and DoDD 8470.01E which established the DoD ESI as the DoD Executive Agent for Core Enterprise Technology Agreements. As the Department's Executive Agent, the DoD ESI has established and offers standard terms and costs and promotes their use across the Department. Further, the DoD ESI provides department-wide guidance and tools to support planning for and establishing software license agreements to minimize the impact of restrictive software licensing practices on cloud computing efforts. The DoD will issue guidance to close the gaps identified in the GAO report, further streamlining and enhancing the procurement process, further leverage DoD ESI best practices, expanding collaboration among stakeholders, and providing a clear definition of restrictive software license practices and their potential risk on cloud computing efforts. The DoD CIO will publish this updated guidance by Q4FY24.

My point of contact for this matter is Mr. Ed Zick who may be reached at (703) 622-8061 or edward.c.zick.civ@mail.mil.

John B. Sherman

Accessible Text for Appendix II: Comments from the Department of Defense

Ms. Carol C. Harris, Director, Information Technology, Management Issues
U.S. Government Accountability Office
441 G Street, NW, Washington, DC 20548

Dear Ms. Harris,

This is the Department of Defense (DoD) response to the Government Accountability Office (GAO) Draft Report, GAO-23-106290, "DOD Software Licenses: Better Guidance and Plans Needed to Ensure Restrictive Practices are mitigated," dated July 2023 (GAO Code 106290).

RECOMMENDATION 1: The GAO recommends that the Secretary of Defense direct the DoD ChiefInformation Officer (CIO), in coordination with Enterprise Software Initiative (ESI), to update and implement guidance and plans to fully address identifying, analyzing, and mitigating the impacts of restrictive software licensing practices on cloud computing efforts.

DoD RESPONSE: Concur. DoD acknowledges the significance of managing and implementing software licensing best practices to minimize the impact of software license restrictions when deploying software within cloud environments. The DoD has various policies in place that guides information technology acquisition including the recent update to DoDI 5000.82 "Requirements for the Acquisition of Digital Capabilities" and DoDD 8470.0IE which established the DoD ESI as the DoD Executive Agent for Core Enterprise Technology Agreements. As the Department's Executive Agent, the DoD ESI has established and offers standard terms and costs and promotes their use across the Department. Further, the DoD ESI provides department-wide guidance and tools to support planning for and establishing software license agreements to minimize the impact of restrictive software licensing practices on cloud computing efforts. The DoD will issue guidance to close the gaps identified in the GAO report, further streamlining and enhancing the procurement process, further leverage DoD ESI best practices, expanding collaboration among stakeholders, and providing a clear definition of restrictive software license practices and their potential risk on cloud computing efforts. The DoD CIO will publish this updated guidance by Q4FY24.

My point of contact for this matter is Mr. Ed Zick who may be reached at (703) 622-8061 or edward.c.zick.civ@mail.mil.
John B. Sherman

Appendix III: GAO Contact and Staff Acknowledgments

GAO Contact

Carol C. Harris, (202) 512-4456, or HarrisCC@gao.gov

Staff Acknowledgments

In addition to the contact named above, Niti Tandon (Assistant Director), Amanda Gill (Analyst in Charge), Amanda Andrade, Rebecca Eyler, Matthew Gray, Franklin Jackson, Ashley Paw, Andrew Stavisky, and Adam Vodraska made key contributions to this report.

GAO's Mission

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

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through our website. Each weekday afternoon, GAO posts on its website newly released reports, testimony, and correspondence. You can also subscribe to GAO's email updates to receive notification of newly posted products.

Order by Phone

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

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

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

Connect with GAO

Connect with GAO on Facebook, Flickr, Twitter, and YouTube.
Subscribe to our RSS Feeds or Email Updates. Listen to our Podcasts.
Visit GAO on the web at https://www.gao.gov.

To Report Fraud, Waste, and Abuse in Federal Programs

Contact FraudNet:

Website: https://www.gao.gov/about/what-gao-does/fraudnet

Automated answering system: (800) 424-5454 or (202) 512-7700

Congressional Relations

A. Nicole Clowers, Managing Director, ClowersA@gao.gov, (202) 512-4400, U.S. Government Accountability Office, 441 G Street NW, Room 7125, Washington, DC 20548

Public Affairs

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

Strategic Planning and External Liaison

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

Please Print on Recycled Paper.