

Artificial Intelligence: Actions and Opportunities to Implement Responsible Use in DOD

GAO-27-107837

Q&A Report to Congressional Committees

October 14, 2026

Why This Matters

Artificial intelligence (AI) has changed the national security landscape. U.S. adversaries and competitors are investing heavily in AI and AI-enabled capabilities in ways that threaten global security, peace, and stability. In January 2026, the Department of Defense (DOD) issued the *Artificial Intelligence Strategy for the Department of War, Accelerating America's Military AI Dominance*—which seeks to prioritize speed in accelerating AI development across the department. As DOD speeds AI development, it is critical for the department to do so responsibly so that warfighters can quickly and confidently adopt it.

Senate Report 118-188 accompanying a bill for the National Defense Authorization Act for Fiscal Year 2025 includes a provision for us to review the implementation and oversight of DOD's responsible AI guidance, among other things (S. Rep. No. 118-188, at 76-77 (2024)). This report discusses DOD's approach to the responsible use of AI, including related guidance, implementation, and oversight.

Key Takeaways

- DOD established the concept of Responsible AI as its approach to ensuring the safety and trustworthiness of AI systems, with a goal of speeding AI adoption while adhering to lawful and ethical principles.
- The Chief Digital and Artificial Intelligence Officer (CDAO) has principal responsibility for AI development and deployment department-wide, including oversight of Responsible AI implementation.
- Since 2022, the CDAO has supported Responsible AI implementation, but faces collaboration and workforce challenges.
- We recommend that the CDAO define roles, responsibilities, and meeting frequency for its collaborative forum to discuss and resolve Responsible AI issues; and take action to address Responsible AI workforce needs to help meet DOD's desired objectives for Responsible AI. We also recommend that Congress consider directing DOD to implement our prior recommendations on similar AI-related issues across the department.

How does DOD define and use AI?

According to DOD, AI refers to the ability of machines to perform tasks that normally require human intelligence—for example, recognizing patterns, learning from experience, drawing conclusions, making predictions, or taking action—whether digitally or as the smart software behind autonomous physical systems.¹ Figure 1 describes the general ways in which DOD is developing, integrating, and supporting AI in the department.

Figure 1: Descriptions and Examples of DOD Artificial Intelligence (AI) Activities by Category

Category	Description	Example(s)
 AI Development	Activities that build and mature AI models, algorithms, and concepts that result in a capability that can be used in a system	• Training deep learning models for automated target recognition • Conducting test and evaluation of AI algorithms to advance unmanned aerial system performance
 AI Integration and Application	Activities that use AI to enable analysis, automation, communication, monitoring, sensing, and other military activities	• Using operational data to fine tune a pre-trained large language model to assist personnel in referencing regulations and protocols
 AI Support	Activities that promote the development, deployment, and use of AI to be faster, scalable, and more responsible	• Delivering a toolkit to help teams develop, test, evaluate, and monitor AI capabilities responsibly

Source: GAO analysis of Department of Defense (DOD) information. | GAO-27-107837

Note: According to DOD Instruction 5000.61, a model is a physical, mathematical, or otherwise logical representation of a system, entity, phenomenon, or process.

A specific scenario where AI is employed is known as a “use case.”² For example, DOD’s Maven, established in 2017 as a flagship AI project, automatically detects, identifies, characterizes, extracts, and attributes features and objects in imagery and video. This helps military commands locate objects and direct analysts to abnormal or significant activity in near real time.

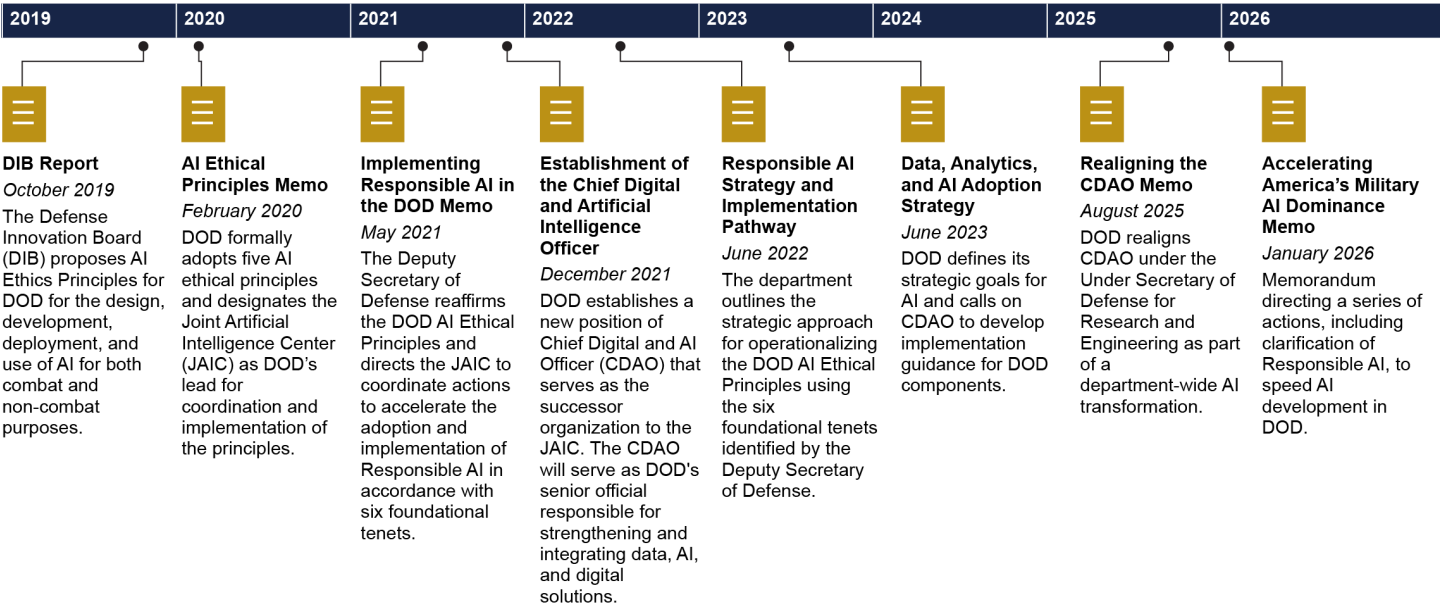
AI use cases we examined from selected DOD components (such as the military services and defense agencies) included automatic target recognition and agentic AI, among others (see app. I for more details).³ As of February 2026, CDAO officials said that DOD reported 378 AI use cases across the department.⁴

What is Responsible AI?

Responsible AI is DOD’s dynamic approach to the design, development, deployment, and use of AI systems that implements DOD AI Ethical Principles to advance the trustworthiness of AI systems. According to DOD’s 2022 *Responsible AI Strategy and Implementation Pathway (Pathway)*, Responsible AI fosters trust and accuracy to overcome uncertainty and hesitancy and thereby speed AI adoption.⁵

Responsible AI has evolved through a series of guidance documents since 2019 (see fig. 2).

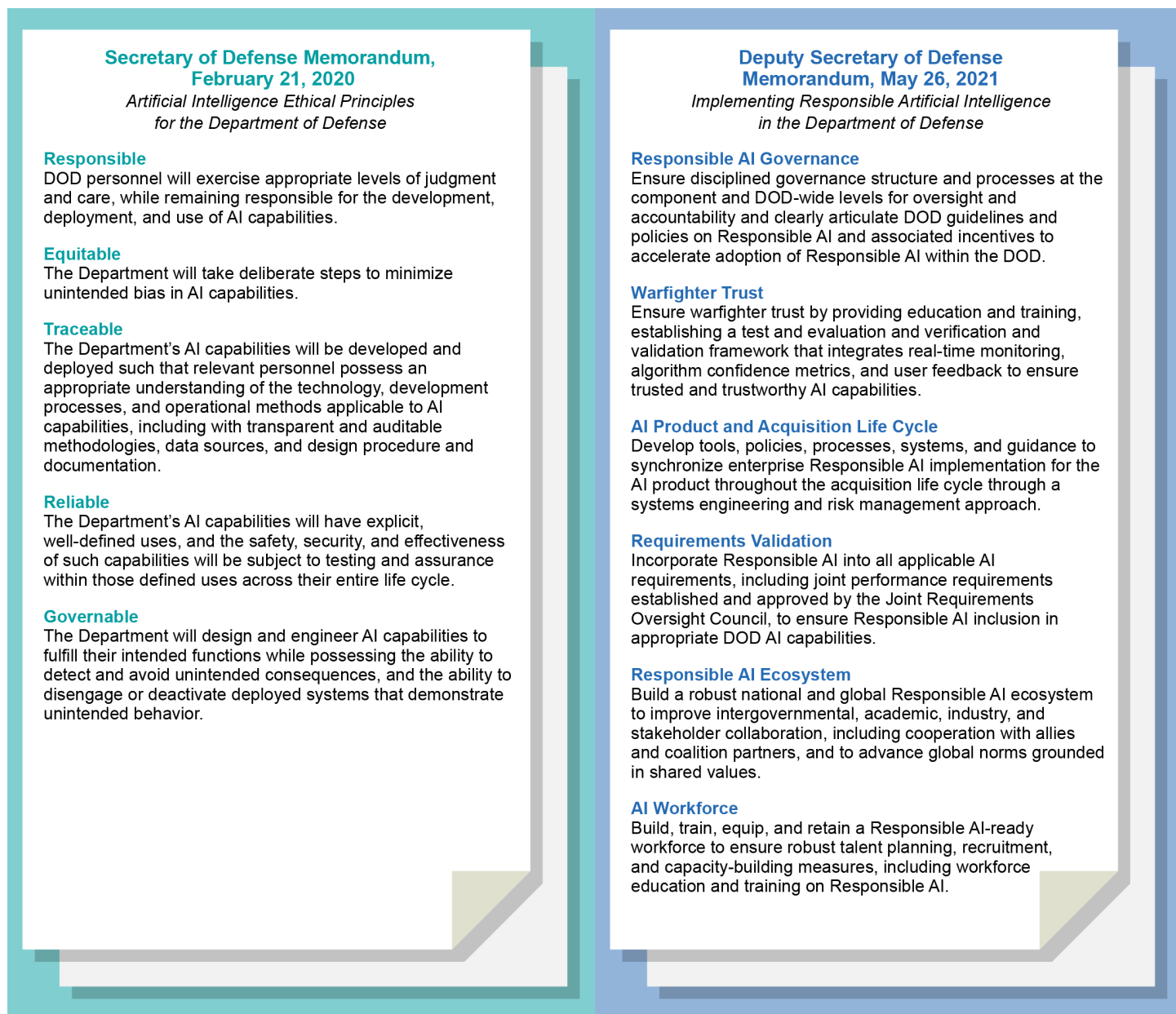
Figure 2: Timeline of DOD Artificial Intelligence (AI) Events and Guidance



Source: GAO analysis of Department of Defense (DOD) information. | GAO-27-107837

DOD adopted its AI Ethical Principles in a February 2020 Secretary of Defense memorandum.⁶ Subsequently, in a May 2021 memorandum, the Deputy Secretary of Defense reaffirmed DOD's AI Ethical Principles and established the department's approach to incorporating those principles in Responsible AI.⁷ The memorandum defined six priority areas, or foundational tenets, to guide DOD's Responsible AI implementation (see fig. 3).

Figure 3: Definitions of DOD Artificial Intelligence (AI) Ethical Principles and Responsible AI Tenets



Source: GAO summary of Department of Defense (DOD) documents. | GAO-27-107837

DOD further defined these tenets and identified 64 lines of effort to guide Responsible AI implementation in the *Pathway*. The lines of effort were aimed at, among other things, developing the tools, processes, and resources necessary for incorporating the DOD AI Ethical Principles into each stage of the AI life cycle. The *Pathway* organized the efforts by their connection to the Responsible AI tenets and assigned them to DOD organizations and offices. In 2023, DOD issued its *Data, Analytics, and Artificial Intelligence Adoption Strategy*, which supported Responsible AI through effective enterprise data governance to achieve increased data quality and insightful analytics.

Most recently, in January 2026, the Secretary of Defense's *Artificial Intelligence Strategy for the Department of War* memorandum re-emphasized accelerating AI integration and adoption. The strategy established new timelines for AI development and directed the department to use metrics that assess the impact of new AI capabilities on mission. The strategy emphasized a wartime footing,

calling for DOD to become an “AI first” warfighting force across all components. The strategy clarified that Responsible AI is to utilize models free from usage policy constraints that may limit lawful military applications and emphasized AI model objectivity as a primary procurement criterion.

Who in DOD implements Responsible AI?

As of January 2026, DOD guidance assigns roles and responsibilities related to Responsible AI implementation to the CDAO and DOD components. Office of the CDAO officials told us the department uses a federated, collaborative approach to promote Responsible AI (for the purposes of this report, hereafter CDAO refers to either the officer or the office). Specifically, the *Pathway* assigns the CDAO a centralized role in providing Responsible AI guidance and policies while it decentralizes the implementation of Responsible AI by assigning execution to the components.

- **CDAO.** According to the *Pathway*, the CDAO is to lead all matters related to DOD adoption and integration of AI, including Responsible AI and the DOD AI Ethical Principles. The CDAO has primary policy oversight responsibility for developing and deploying AI, according to DOD’s chartering directive titled *Chief Digital and Artificial Intelligence Officer*.⁸ The CDAO is also the department’s principal officer responsible for AI strategic guidance and services—like training—that support DOD components’ development and deployment of AI.⁹ Three offices within CDAO play significant roles in Responsible AI:
 - **Responsible AI Division.** According to CDAO officials this division was tasked with accelerating AI adoption by building trust via rigorous assessment, test and evaluation, and monitoring—while also streamlining policy/regulatory barriers.
 - **Policy Branch.** According to CDAO officials, the Policy Branch plans to develop new or adjust existing AI policy, in accordance with executive branch guidance. Officials said the branch is using policy “sandboxes”—which are interagency efforts—that assess AI use cases against existing DOD policy to find policy gaps, risks, and issues with safety or performance.
 - **Capabilities and Development Branch.** CDAO officials told us that this branch plans to enable Responsible AI policy development by gathering and sharing lessons learned across DOD from Responsible AI tools and best practices.
- **DOD components.** The *Pathway* assigns DOD components responsibilities for specific lines of effort to implement Responsible AI. Further, the *Pathway* states that DOD components will identify the resources and appropriate personnel, expertise, and experience to carry out these lines of effort. According to CDAO officials, one of the first lines of effort to be completed was components’ designating or hiring of Responsible AI leads to support implementation of the other lines of effort. DOD’s *Data, Analytics, and Artificial Intelligence Adoption Strategy*, which highlights the need to responsibly and rapidly realize the full promise of data, analytics, and AI, directs components to implement the strategy according to self-assessed maturity levels, mission parameters, and pertinent laws.¹⁰

Since 2018, DOD has restructured and realigned the organizations responsible for implementing AI and leading Responsible AI within the department. In August 2025, DOD realigned the CDAO under the Under Secretary of Defense for Research and Engineering.¹¹ Previously, the CDAO reported directly to the Deputy Secretary of Defense and, through this deputy, to the Secretary of Defense, per December 2021 guidance.¹²

The CDAO is the successor organization to the Joint Artificial Intelligence Center, which was disestablished in 2022.¹³ From 2018 to 2021, the Joint Artificial Intelligence Center facilitated the development of DOD’s AI governance, standards, ethics, and cybersecurity. Initially, the center reported to the DOD Chief Information Officer. Subsequently, section 232 of the National Defense Authorization Act for Fiscal Year 2021 directed that the Director of the Joint Artificial Intelligence Center report directly to the Deputy Secretary of Defense.¹⁴

How has CDAO supported Responsible AI implementation across DOD?

The CDAO, through the Responsible AI Division, has led collaborative groups, developed Responsible AI tools and guidance, and conducted technical engagements to support Responsible AI implementation.

Collaborative groups. CDAO’s Responsible AI Division leads the Responsible AI Working Council. According to the *Pathway*, this council serves as a permanent working group to receive reports on DOD components progress implementing the *Pathway* as well as identifying relevant barriers to AI adoption for removal. In addition, the Responsible AI Division leads the federal Chief AI Officers Council’s AI Assurance Working Group, which recommended processes and resources for meeting federal AI risk management requirements.¹⁵ The Responsible AI Division also co-chairs the North Atlantic Treaty Organization Data and AI Review Board’s subgroup on AI Assurance.

Tools and guidance. In 2023, CDAO released the Responsible AI Toolkit. The toolkit provides a centralized process that identifies, tracks, and improves the alignment of AI projects toward Responsible AI best practices and DOD’s AI Ethical Principles. According to DOD, its flow guides users through tailorable and modular assessments, tools, and artifacts throughout the AI product life cycle. According to CDAO officials, the Responsible AI Toolkit has been used by at least four DOD components and is being piloted elsewhere.

According to CDAO officials, they also worked with other organizations to develop related tools. In October 2023, the North Atlantic Treaty Organization adopted a version of DOD’s Responsible AI Toolkit that was customized for their principles of responsible use, according to CDAO officials. Further, in September 2025 the federal Chief AI Officers Council—which coordinates AI innovation and governance across the federal government—issued an AI Minimum Risk Management Resources document that includes a toolkit, based in part on the DOD Responsible AI Toolkit.¹⁶ Table 1 shows selected examples of other CDAO tools.

Table 1: Selected Examples of Chief Digital and Artificial Intelligence Officer (CDAO) Responsible Artificial Intelligence (AI) Implementation Tools	
Tool	Tool description
DOD AI Guide on Risk	A checklist to calculate, document, and mitigate risks for an AI. Also helps keep senior leaders informed on responsibility and traceability.
Large Language Model Benchmark Test Harness	Automatically generates, validates, and runs benchmarks for DOD use cases, allowing users to assess potential bias.
Human Machine Red Teaming	Adapts proven red teaming process for assessing human-AI teaming technologies.

Source: GAO analysis of Department of Defense (DOD) information. | GAO-27-107837

Note: The Large Language Model Benchmark Test Harness and the Human Machine Red Teaming tools were developed for CDAO by federally funded research and development centers.

In addition to the *Pathway* and guidance included in the toolkit, CDAO Responsible AI Division authored other key guidance, including the July 2024

memorandum: *DOD Guidelines and Guardrails to Inform Governance of Generative Artificial Intelligence*.¹⁷ To produce this memorandum, the Responsible AI Division led seven DOD-wide research groups that examined issues such as data quality, cyber and adversary threats, and traceability, according to CDAO officials.

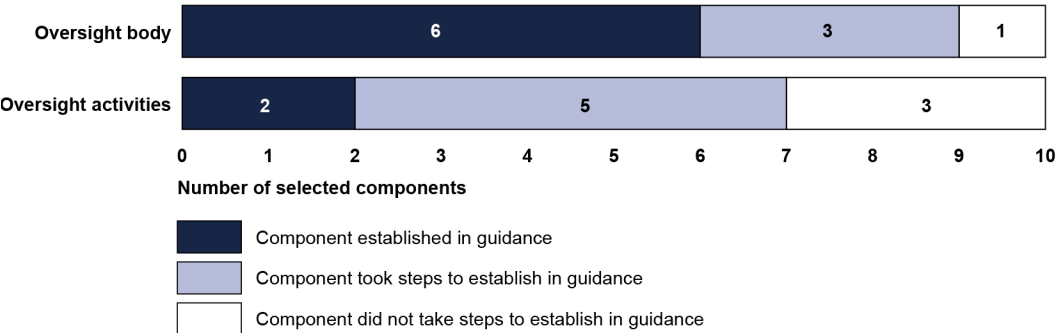
Technical exchanges. CDAO’s Responsible AI Division also led technical exchanges and meetings. For example:

- In October 2024, the Responsible AI Division assisted CDAO in hosting a forum on Responsible AI in DOD. The forum included defense leaders, industry partners, AI experts, and AI policy makers.
- In December 2024, the Responsible AI Division led a crowdsourced effort to use adversarial techniques to test large-language model chatbots in the context of military medicine. The effort crowdsourced input from over 200 participants, including clinical providers and health care analysts from the Defense Health Agency, the Uniformed Services University of the Health Sciences, and the military services.
- The Responsible AI Division is collaborating with other CDAO offices and the National Cyber Range Complex to establish cyber test ranges where industry partners can test pre-release AI models on representative DOD infrastructure. DOD intends to evaluate models and capabilities using these test ranges and thereby speed deployment of AI.

How are selected DOD components implementing Responsible AI?

Most of the 10 DOD components we surveyed have taken at least initial steps to establish oversight and implement Responsible AI tenets in their respective use cases. Nine of 10 selected components have either established or taken steps to establish oversight bodies in guidance and seven of 10 have taken steps to establish oversight activities in guidance to varying degrees (see fig. 4).

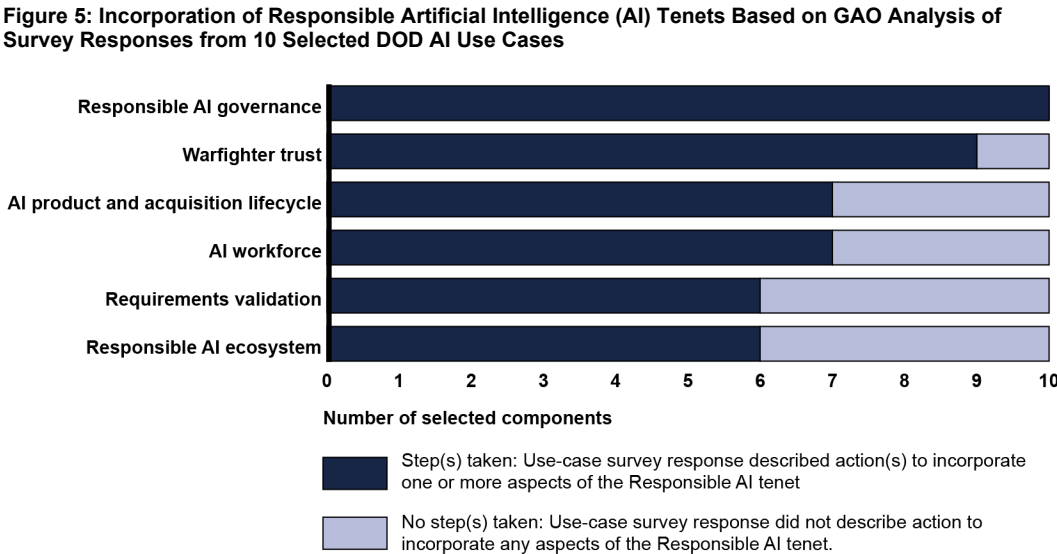
Figure 4: Selected DOD Components’ Establishment of Responsible Artificial Intelligence (AI) Oversight Structures



Source: GAO analysis of Department of Defense (DOD) information. | GAO-27-107837

Our analysis of the components’ survey responses showed all 10 components took steps to incorporate at least one tenet (Responsible AI Governance) in the selected use cases that comprised our nongeneralizable sample. Figure 5 shows the numbers of component use cases that we assessed to have provided information, via their survey responses, of having taken steps to incorporate each tenet in their respective use cases. For example, we assessed that the information in the Army’s survey response demonstrated that steps had been taken to incorporate the AI Product and Acquisition Life Cycle tenet. This was because the survey response described the establishment of data standards and associated required documentation for the data providers working on their AI-aided automatic target recognition program. In the Navy use case, we assessed that Navy had not taken steps to incorporate the Requirements Validation tenet because use case officials responded “no” to yes/no questions asking whether

the requirements for their AI were aligned with Responsible AI tenets. The survey response noted that Requirement Validation plans were in development.¹⁸ See appendixes I, II, and III for information about the selected AI use cases and survey analysis results.



Source: GAO analysis of Department of Defense (DOD) information. | GAO-27-107837

Responsible AI implementation looks different across DOD components. According to CDAO officials, some components use CDAO resources, such as the CDAO Responsible AI Toolkit, while others rely on their own tools. According to CDAO documentation, its toolkit was used by U.S. Army Special Operations Command, the Navy, the Army, and the National Geospatial-Intelligence Agency. In December 2025, the Responsible AI Division integrated the toolkit into the Maven Smart System. The toolkit is also being piloted with other offices within U.S. Transportation Command, the National Geospatial-Intelligence Agency, and the Navy.

Our analysis of DOD components' survey responses showed that some components implemented Responsible AI tenets using their own advanced planning or automated processes. For example, the Defense Intelligence Agency published a Quality Assurance Framework in fiscal year 2024 that establishes an accreditation program with a series of steps for AI owners to complete, such as documentation and key milestones for building Responsible AI systems, according to agency officials.¹⁹ The guidance also identifies an office responsible for AI oversight.

To what extent do CDAO and DOD components collaborate on Responsible AI?

CDAO and DOD components have taken steps to collaborate as they implement Responsible AI. For example, CDAO officials told us that they collaborated with components to develop guidance in the *Pathway*, coordinate its finalization, and establish Responsible AI leads.²⁰ As previously noted, CDAO also leads and participates in a variety of collaborative forums. DOD components provided examples of collaboration in their survey responses. However, we identified limitations in CDAO's primary collaborative organization—its Responsible AI Working Council—that could affect the timing and efficiency of the department's Responsible AI implementation.

Responsible AI Working Council

Since May 2021, DOD has used the Responsible AI Working Council as the permanent working-level collaborative group for Responsible AI. However, recently the council has been limited in providing regular, formal opportunities for

collaboration. CDAO officials acknowledged that the council did not meet from late 2024 until August 2025. Prior to the lapse in Responsible AI Working Council meetings, CDAO officials said monthly meetings on Responsible AI were held with department-wide attendance. However, CDAO officials said that other priorities limited their ability to organize council meetings for a period of time. Specifically, a July 2024 CDAO memorandum directed the Responsible AI Division to develop a toolkit for generative AI. The division leadership also supported a government-wide Chief AI Officer Council effort to develop *AI Minimum Risk Management Resources*, published in September 2025.²¹ Officials from the Responsible AI Division said this work prevented them from organizing meetings for the Responsible AI Working Council.

In interviews, officials from four DOD components told us they faced Responsible AI implementation challenges during this time period that would have benefited from collaboration. For example, officials from Joint Staff said that they previously used the council to coordinate completion of the lines of effort from the *Pathway*, and faced challenges with this coordination during the council's lapse in meetings. Officials from the Defense Threat Reduction Agency said they wanted more collaboration with CDAO and other DOD components on how to consistently interpret federal guidance and apply Responsible AI to high-impact use cases.

Officials from the Air Force noted that during the time period when the council did not meet, they began building their own Responsible AI governance structure and processes but were challenged in getting practices for doing so from other components. These officials said that they instead relied on Air Force use cases to implement Responsible AI themselves. Air Force and Defense Threat Reduction Agency officials said they collaborated informally on an ad hoc basis. The Navy also started to build its own Responsible AI governance structure and wanted to collaborate with other components to validate its efforts, according to Navy officials.

The *Pathway* states that the CDAO is responsible for centralized, DOD-wide Responsible AI coordination. It further states that the Responsible AI Working Council should update its membership to reflect the designated Responsible AI leads in components, formalize its role through a charter approved by the CDAO, and assist the CDAO in reporting on the progress of DOD-wide Responsible AI implementation. DOD's 2023 *Data, Analytics, and AI Adoption Strategy* also emphasizes the importance of CDAO's use of collaborative forums, noting their value in addressing issues with developing data quality to address AI requirements.²²

However, the Responsible AI Working Council does not have a charter with assigned roles, responsibilities, and meeting frequency. CDAO officials acknowledged not having a charter and said that the initial direction for the council came from the May 2021 Deputy Secretary of Defense memorandum, which directed the council to complete several tasks including drafting the *Pathway*. Further, these officials noted that after the 2024–2025 hiatus, the Responsible AI Working Council resumed meetings in August 2025. However, DOD's January 2026 memorandum *Artificial Intelligence Strategy for the Department of War* clarified the definition and scope of Responsible AI and directed CDAO to ensure all existing AI policy guidance at the department aligns with the directives laid out in the memorandum. According to officials from the Responsible AI Division, they have been charged with this task. Without a charter that defines roles and responsibilities for the council in light of the most recent AI strategy, and that specifies the frequency of council meetings, the council is at risk of lapsing again. Such a lapse could increase the risk of DOD facing

Responsible AI implementation issues that it would not have the collaborative capacity to swiftly and effectively resolve.

By taking steps to formalize the Responsible AI Working Council as a collaborative forum for problem solving, CDAO could improve components' experience with implementing Responsible AI and help them resolve challenges. In the next question we discuss reported and potential benefits of such collaboration.

Open recommendation from past work

DOD also has not fully addressed an open recommendation from our past work that addressed, among other things, collaboration in AI adoption across DOD.²³ In 2022 we reported that DOD did not have performance measures and milestones to achieve outcomes for AI collaboration; some DOD officials were unaware of DOD AI-related efforts to reduce fragmentation; and DOD did not define or set expectations for those responsible for collaborating on AI. We concluded that unless DOD addressed these shortcomings through collaboration, it risked having a fragmented approach that could lead to unnecessary duplication and overlap. As noted above, DOD has faced collaboration challenges with Responsible AI; moreover, multiple past changes in the structure and alignment of CDAO and its predecessor organizations amplify the need to document roles and responsibilities. We recommended that DOD define the roles and responsibilities of the military services and other DOD organizations for leadership and relevant participants collaborating on AI activities.

As of May 2026, this recommendation remains open. Fully addressing our prior recommendation would help DOD ensure its approach to adopting and integrating AI technologies is not unnecessarily fragmented and that it is effectively leveraging expertise to meet its desired objectives for AI across the department.

What are some of the reported and potential benefits of collaboration?

Our analysis of survey results identified both reported and potential benefits of collaboration on Responsible AI implementation.²⁴ In response to our nongeneralizable survey, six of 10 selected components reported that collaboration with other organizations in their development of AI use cases led to positive outcomes.²⁵ For example:

- The Air Force reported collaboration with a variety of DOD components was critical to its use case team's understanding of performance data and efforts to define relevant metrics, design algorithm experiments, and provide model evaluation tools.
- The National Geospatial-Intelligence Agency reported that for its use case, collaboration across DOD created an environment of increased trust and the ability of the program to rapidly respond to warfighter needs while ensuring adherence to development and testing standards.

In addition, six of 10 selected components responded that sharing Responsible AI resources and best practices would increase their organization's ability to incorporate the six Responsible AI tenets into their AI use case.²⁶

In our analysis of survey results and related interviews, we also found additional instances in which components reported challenges that could potentially be addressed through collaboration with other DOD components. Table 2 describes examples of challenges reported by components in survey results and related interviews, and related practices reported by other components that we determined could be beneficial if shared.

Table 2: Examples of DOD Components’ Responsible Artificial Intelligence (AI) Implementation Challenges and Related Practices

Reported component challenge	Potentially related practice
Defense Threat Reduction Agency officials stated in an interview that the Chief Digital and Artificial Intelligence Office’s Responsible Artificial Intelligence (AI) Toolkit did not have metrics to track progress.	The National Geospatial-Intelligence Agency use-case survey response reported that it has developed Test and Evaluation metrics for its AI use cases that could potentially be adopted by other components.
The Air Force use-case survey response stated that industry partners’ proprietary AI models lacked transparency in data, algorithms, or model characteristics, which hindered an objective assessment of responsible AI implementation.	Defense Intelligence Agency officials said in an interview that development of a Quality Assurance Framework that describes how transparency for the user of the AI (transparency of where the source material came from, the confidence level of the algorithm, etc.) should be included in AI systems.
Marine Corps use-case survey response stated that Responsible AI tools were not available in the classified environment.	Special Operations Command use-case survey response noted that it adapted its general classified environment accreditation process to Responsible AI.

Source: GAO analysis of Department of Defense (DOD) survey information. | GAO-27-107837

Note: The examples presented here are from GAO’s nongeneralizable survey and related interviews. As such, they are illustrative examples of reported challenges that align with reported practices that could potentially mitigate those challenges. They do not represent any trends across DOD.

What additional actions for implementing Responsible AI has DOD identified and what challenges does DOD face in taking them?

CDAO officials stated that taking the following actions could help DOD implement Responsible AI:

- Operationalizing CDAO’s oversight role through mechanisms whereby officials could monitor AI projects for implementation of the Responsible AI tenets. According to the *Pathway*, CDAO is responsible for enabling, assessing, and tracking the implementation of the DOD Responsible AI ecosystem with support from the components.
- Evaluating the usage and effectiveness of the Responsible AI toolkit and other best practices before requiring usage of the Responsible AI tools and practices. According to a 2024 draft unpublished DOD report on the state of Responsible AI, CDAO was to undertake several validation efforts assessing best practices, tools, and policies.²⁷
- Completing the remaining lines of effort from the *Pathway*. For example, the *Pathway* directs CDAO to develop metrics to measure Responsible AI adoption, including progress on individual lines of effort, and to report progress to the CDAO governing council. While CDAO has been tracking implementation of the lines of efforts, it has not developed metrics to measure implementation of Responsible AI. According to CDAO officials, many lines of effort assigned to DOD components are also incomplete. As of April 2026, CDAO documentation showed that 29 of 64 lines of effort were incomplete.

CDAO’s Responsible AI workforce challenge

However, according to officials, CDAO has experienced staffing shortages that have hindered its ability to take these actions. CDAO officials said that a 2023 resourcing memorandum authorized CDAO 10 positions for Responsible AI, including a Systems Engineer, a Program Manager, and an AI Ethicist, among other positions. But according to CDAO officials, as of February 2026, only three

of the 10 positions are filled and CDAO is unlikely to fill vacant positions or increase staffing. Officials said this is because CDAO is still restructuring as part of its realignment to the Office of the Under Secretary of Defense for Research and Engineering and must take into account the new 2026 DOD *Artificial Intelligence Strategy for the Department of War, Accelerating America's Military AI Dominance*. While this strategy clarifies the definition and scope of Responsible AI, it also assigns specific tasks related to Responsible AI, such as ensuring all DOD existing policy guidance aligns with the directives of the strategy.

The first line of effort in the *Pathway* was to fully staff the CDAO Responsible AI office with expertise in AI technology, policy, acquisition, workforce, and governance. Responsible AI enables DOD to more quickly develop and adopt AI as it identifies the critical principles and good engineering to develop trustworthy AI systems. By addressing the current workforce needs for Responsible AI and taking action to ensure it has staff in place to meet those needs, CDAO could further implement Responsible AI and make progress toward achieving its goal of accelerating AI across DOD.

Open recommendations from past work

We previously reported in 2023 on DOD's challenges with AI workforce management. We reported that DOD took some steps to address these, such as conducting a series of interviews with DOD components and defining five AI work roles. However, we found that DOD had not taken critical next steps to fully define and identify its AI workforce. For example, DOD had not coded AI work roles into its workforce data systems, updated guidance, or developed a qualification program. We made three recommendations, including for DOD to (1) assign responsibility and (2) establish a timeline to complete the steps necessary to fully define and identify DOD's AI workforce.²⁸ As of May 2026, these two recommendations remain open. Our third recommendation, for DOD to update its Human Capital Operating Plan to address AI workforce issues, is partially addressed.

Addressing these AI workforce issues, as well as our open recommendation from 2022 on defining the roles of participants collaborating on AI activities, will be of critical importance as DOD accelerates AI adoption across the department. Our 2022 report noted that incorporating leading practices for collaboration can improve an agency's efforts to achieve its desired outcomes. Our 2023 report highlighted DOD guidance, as well as federal regulation and Office of Personnel Management guidance, on the importance of workforce management for supporting the DOD mission.

Ensuring that DOD is actively taking steps to fully address our prior recommendations on AI collaboration and workforce management would help both Congress and DOD ensure that the entire department is well positioned to meet its AI acceleration goals.

Conclusions

Incorporating Responsible AI tenets throughout the AI life cycle is critical to DOD's ability to speed AI capability development and adoption in a changing national security landscape. As AI capabilities evolve, continued collaboration among CDAO and DOD components will be important to ensure oversight of and synergy from Responsible AI implementation.

DOD has opportunities to improve its collaborative efforts for AI capabilities. In particular, establishing a charter for the Responsible AI Working Council that specifies roles and responsibilities and the frequency of meetings for the council

would help ensure it functions effectively as a collaborative forum to discuss and resolve component issues with Responsible AI.

Moreover, DOD has opportunities to more effectively manage its workforce to implement Responsible AI. As DOD realigns CDAO under the Under Secretary of Defense for Research and Engineering, it has an opportunity to fulfill the staffing needed for Responsible AI within CDAO.

Finally, given that the department is seeking to accelerate AI with new timelines and broad scope across all of DOD, including warfighting, it will be important for DOD to address identified general AI issues that affect its implementation of Responsible AI. Specifically, addressing our 2022 recommendation on AI collaboration would help DOD ensure it is effectively leveraging expertise to meet its desired objectives for AI; and addressing our 2023 recommendations related to DOD's AI workforce management would be useful for DOD to more effectively assess its overall AI workforce needs, including supporting Responsible AI implementation. Congressional action to ensure that DOD is actively taking steps to address our prior recommendations on AI collaboration and workforce management would help both Congress and DOD ensure that the entire department is well positioned to meet its AI acceleration goals.

Matter for Congressional Consideration

Congress should consider directing DOD to implement our open recommendations on collaboration and the AI workforce, including to (1) define the roles and responsibilities of DOD organizations and components collaborating on AI activities and (2) address AI workforce challenges across the department by assigning responsibility and establishing a timeline for completing steps to fully define and identify DOD's AI workforce.

Recommendations for Executive Action

We are making the following two recommendations to DOD:

The Secretary of Defense should ensure that the Chief Digital and Artificial Intelligence Officer develops and issues a charter for the Responsible AI Working Council that outlines roles and responsibilities and that includes the CDAO's Responsible AI Division (or equivalent office) and DOD components and that specifies the frequency of council meetings. (Recommendation 1)

The Secretary of Defense should ensure that the Chief Digital and Artificial Intelligence Officer addresses the Responsible AI Division's workforce needs. (Recommendation 2)

Agency Comments

We provided a draft of this report to DOD for review and comment. The Department provided comments via email indicating concurrence with both of our recommendations.

How GAO Did This Study

We reviewed Department of Defense (DOD) documentation related to Responsible Artificial Intelligence (AI). For example, we reviewed guidance, such as the May 2021 Deputy Secretary of Defense memorandum on *Implementing Responsible AI in DOD*;²⁹ policy memorandums and directives, including the DOD directives that established the Chief Digital and Artificial Intelligence Officer (CDAO),³⁰ and then moved it under the Under Secretary of Defense for Research and Engineering;³¹ and plans and strategies, including the 2022 *Responsible Artificial Intelligence Strategy and Implementation Pathway*.³² We analyzed these documents to ascertain key definitions (i.e., AI and Responsible AI); organizational oversight roles, responsibilities, and authorities; and desired goals and outcomes of Responsible AI.

We conducted interviews with cognizant DOD officials from CDAO, the military services, and other DOD components about how they incorporate Responsible AI into their AI use cases, including any component practices or challenges. We also inquired about how the components collaborate and the extent to which they are supported by CDAO through guidance, policy, tools, and collaborative groups.

To support the above lines of inquiry and analysis, we also conducted a nongeneralizable survey of 10 DOD components (Army, Navy, Air Force, Space Force, Marine Corps, Defense Intelligence Agency, National Geospatial-Intelligence Agency, Defense Threat Reduction Agency, U.S. Special Operations Command, and U.S. Cyber Command) to understand how they have implemented Responsible AI tenets in 10 selected AI use cases (one per component). We identified potential use cases from a January 2025 CDAO inventory list of 378 AI use cases. Using information in the inventory and discussions with officials from the selected components, we then selected one use case from each component based on the type of AI being developed, the development phase, the intended usage, and other qualitative factors. Appendix III provides details on our methodology for the survey and analysis of the survey responses.

We conducted this performance audit from September 2024 to October 2026 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.

List of Addressees

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

The Honorable Mitch McConnell
Chair
The Honorable Christopher Coons
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
Chairman
The Honorable Betty McCollum
Ranking Member
Subcommittee on Defense
Committee on Appropriations

GAO Contact Information

For more information, contact: Alissa H. Czyz, Director, Defense Capabilities and Management, czyza@gao.gov.

Media Relations: Sarah Kaczmarek, Managing Director, Media@gao.gov.

Congressional Relations: David Powner, Managing Director, dpowner@gao.gov.

Staff Acknowledgments: Penney Harwell Caramia (Assistant Director), Usman Ahmad (Analyst in Charge), Tracy Barnes, Ashley Gavin, Carly Gerbig, Amie Lesser, Clarice Ransom, Michael Silver, Anne Thomas, James Walters.

Connect with GAO on [Facebook](#), [X](#), [LinkedIn](#), [Instagram](#), and [YouTube](#).
Subscribe to our [Email Updates](#). Listen to our [Podcasts](#).

Visit GAO on the web at <https://www.gao.gov>.

This is a work of the U.S. government but may include copyrighted material. For details, see <https://www.gao.gov/copyright>.

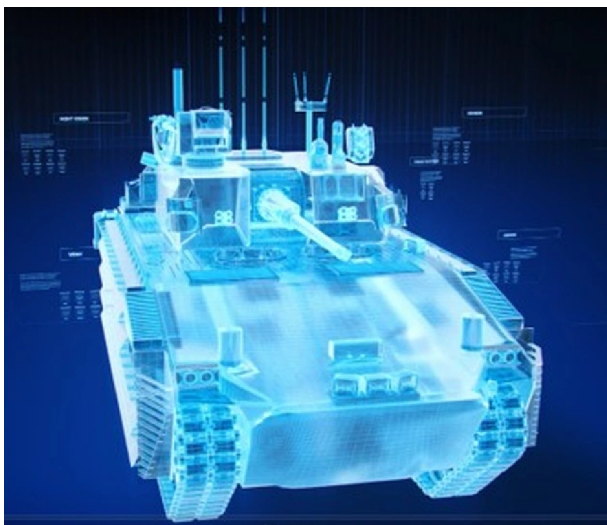
Appendix I: Selected AI Use Cases

We surveyed 10 Department of Defense (DOD) components about their selected artificial intelligence (AI) use cases' implementation of Responsible AI. Information about each selected AI use case, per component, is described in figures 6 through 15.

We conducted our survey from June 2025 to August 2025 and confirmed that the information presented below was current as of March 2026. Unless otherwise noted, the information presented in the figures represents that time frame.

The figures below use terms related to mission areas and types of AI. Generally, these terms are as follows. Warfighting; for example, AI projects that focus on discovering, testing, and scaling novel ways of fighting with AI-enabled capabilities. Intelligence; for example, AI projects that focus on enhancing either the collection or analysis of all types of intelligence. Automatic target recognition; for example, training a machine-learning program on a set of imagery data to identify specific characteristics of targets. Computer vision; for example, training a machine-learning program to process imagery. Agentic AI; for example, a trained large-language model able to interpret and reason.

Figure 6: Counter Unmanned Aerial System Pilot



Use case: Counter Unmanned Aerial System for the XM30

Component: Army

Manager or developer: Project Manager XM30 and AIOps+. AIOps+ is part of Army's Capability Portfolio Executive Intelligence and Spectrum Warfare.

Mission area: Warfighting

Type of Artificial Intelligence (AI): Automatic Target Recognition

Key capabilities: AIOps+ plans to use AI-enabled sensors to detect and track drone threats to Army ground combat vehicles such as the XM30, which is the Army's next-generation infantry fighting vehicle. The AI will integrate advanced sensors with real-time battlefield data analysis, with the objective of speeding soldier response time.

Intended users: XM30 infantry fighting vehicle and other platforms with aided target recognition.

Source: GAO analysis of Department of Defense information; Savannah Baldwin/PEO Ground Combat Systems (image). | GAO-27-107837

Figure 7: Robotic Autonomous Systems Using Automatic Target Recognition



Use case: Robotic Autonomous Systems Using Automatic Target Recognition

Component: Navy

Manager or developer: Partnership between the Navy's Project Overmatch, Defense Innovation Unit, Chief Digital and Artificial Intelligence Office, and National Geospatial- Intelligence Agency.

Mission area: Warfighting

Type of Artificial Intelligence (AI): Automatic Target Recognition

Key capabilities: According to Navy officials, the AI improves target recognition for multiple autonomous robotic systems. For example, the developed AI is planned to integrate mission, targets, and environmental condition information for unmanned vehicles, command and control, and multi-platform and unmanned team capabilities.

Intended users: To be determined

Source: GAO analysis of Department of Defense information; Specialist N. Strachen/U.S. Army (photo). | GAO-27-107837

Figure 8: Machine Assisted Geospatial Exploitation (MAGE) Automatic Target Recognition



Use case: Machine Assisted Geospatial Exploitation Automatic Target Recognition (MAGE)

Component: Air Force

Manager or developer: Air Force Materiel Command

Mission area: Intelligence

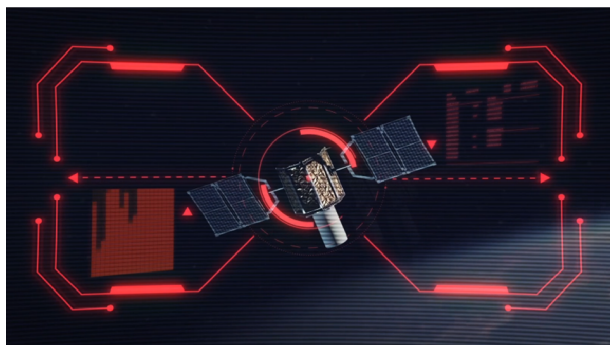
Type of Artificial Intelligence (AI): Automatic Target Recognition

Key capabilities: The AI supports automated target recognition capabilities.

Intended users: Air Force, Intelligence Community, and other commands processing large amounts of intelligence, surveillance, and reconnaissance data.

Source: GAO analysis of Department of Defense information; Air Force Air Combat Command (image). | GAO-27-107837

Figure 9: Counter-Camouflage Concealment Deception Maneuver Classifier



Use case: Counter-Camouflage Concealment Deception Maneuver Classifier

Component: Space Force

Manager or developer: Space Domain Awareness Tools, Applications, and Processing Laboratory

Mission area: Warfighting

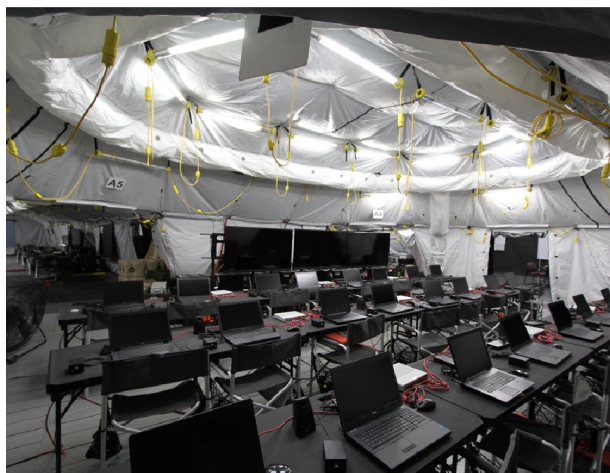
Type of Artificial Intelligence (AI): Computer Vision

Key capabilities: The AI is used to evaluate and classify unknown space objects to uncover hidden threats and enable protection of friendly space capabilities in a crowded space environment. For example, there are hundreds of objects in earth's orbit. Some are harmless debris that should be distinguished from an adversary's concealed kinetic weapon.

Intended users: National Space Defense Center, Joint Commercial Operations, and Space Domain Awareness mission.

Source: GAO analysis of Department of Defense information; R. Isler/Space Systems Command (image). | GAO-27-107837

Figure 10: Artificial Intelligence Support to Operations



Use case: Artificial Intelligence Support to Operations

Component: Marine Corps

Manager or developer: Office of Naval Research (Sponsor/Manager), Naval Research Laboratory, Space Dynamics Laboratory, and Parsons

Mission area: Warfighting

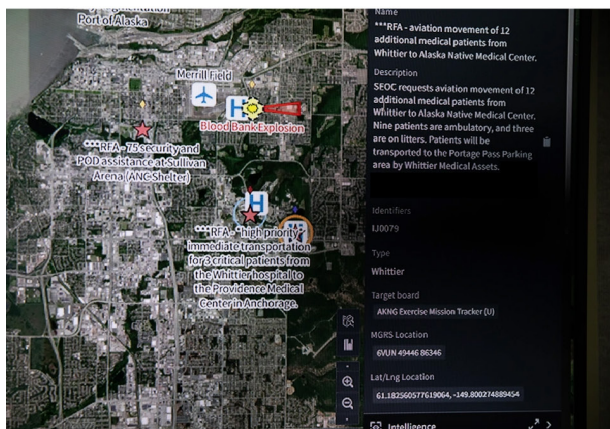
Type of Artificial Intelligence (AI): Agent Network

Key capabilities: The AI is used to improve tactical level decision-making ability when guidance on a high-level tasking by higher echelon units is unavailable. Marine Corps officials said the AI is used within contexts requiring both speed and quality as well as in constrained resource environments.

Intended users: Tactical level ground combat units including battalion level and below.

Source: GAO analysis of Department of Defense information; Lt. M Browne/U.S. Marine Corps (photo). | GAO-27-107837

Figure 11: National Geospatial-Intelligence Agency



Use case: Uses Computer Vision to Product AI Detections

Component: National Geospatial-Intelligence Agency

Manager or developer: Maven Program Office

Mission area: Operations and Intelligence

Type of Artificial Intelligence (AI): Computer Vision

Key capabilities: The AI provides an automated detection capability for objects of military interest in overhead satellite imagery and full motion video.

Intended users: Military and intelligence community analysts.

Source: GAO analysis of Department of Defense information; Staff Sgt. S. LaCount/Alaska National Guard (image). | GAO-27-107837

Figure 12: Detect, Tag, and Track



Use case: Detect, Tag, Track

Component: Defense Threat Reduction Agency

Manager or developer: Research and Development Directorate, Advanced Research for Countering WMD Technologies; Applied Research Associates

Mission area: Warfighting

Type of Artificial Intelligence (AI): Supervised computer vision models for automatic target recognition

Key capabilities: Detect, Tag, Track uses AI to accurately determine if a specific vehicle has been identified and to continually track that vehicle.

Intended users: U.S. Special Operations Command

Source: GAO analysis of Department of Defense information; Defense Threat Reduction Agency (photo). | GAO-27-107837

Figure 13: Collaborative Heterogenous Autonomous Operations Software



Use case: Collaborative Heterogenous Autonomous Operations Software (CHAOS)

Component: Special Operations Command

Manager or developer: Unmanned System Autonomy and Interoperability Program Manager

Mission area: Warfighting

Type of Artificial Intelligence (AI): Automatic Target Recognition and Mission Autonomy

Key capabilities: CHAOS supports autonomous control of unmanned systems that may need to coordinate automatic target recognition and mission autonomy.

Intended users: Special Operations Command, with the possibility of scaling to wider DOD users.

Source: GAO analysis of Department of Defense (DOD) information; Special Operations Command (image). | GAO-27-107837

Figure 14: Redline



Use case: Redline

Component: Defense Intelligence Agency

Manager or developer: Defense Intelligence Agency, Directorate for Analysis, Analytic Innovation

Mission area: Intelligence and Warfighting

Type of Artificial Intelligence (AI): Machine learning target recognition and labeling

Intended users: Supported mission owners and collection managers across the Defense Intelligence Enterprise.

Source: GAO analysis of Department of Defense information; Defense Intelligence Agency (image). | GAO-27-107837

Figure 15: Malware & AI Nexus for Targeted Intelligence Support



Use case: Malware & AI Nexus for Targeted Intelligence Support

Component: Cyber Command

Manager or developer: United States Cyber Command AI Task Force, Johns Hopkins University Applied Physics Lab

Mission area: Warfighting and Intelligence

Type of Artificial Intelligence (AI): Agentic AI system

Key capabilities: The AI is designed to fuse multiple data sources and data analytic techniques into a single chat-based large language model interface.

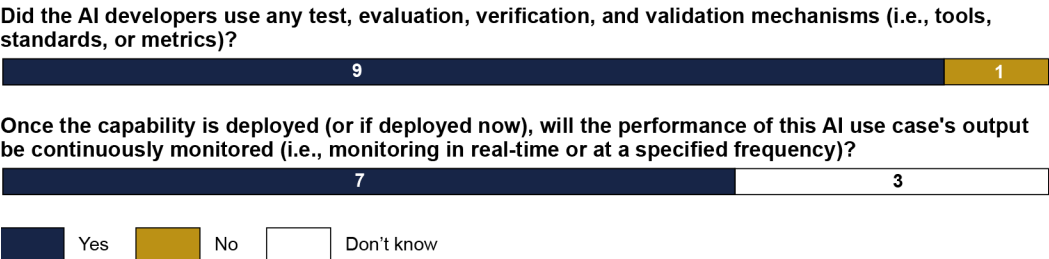
Intended users: Cyber missions

Source: GAO analysis of Department of Defense information; J. Cole/U.S. Cyber Command (photo). | GAO-27-107837

Appendix II: Selected Data Analysis Results from Survey of DOD Components

We conducted a survey of 10 Department of Defense (DOD) components about their Responsible Artificial Intelligence (AI) implementation in specific AI use cases. This appendix highlights selected data analysis results. Figures 16 through 18 and table 3 include the verbatim wording of questions we asked in our survey about DOD Responsible AI tenets, which are Responsible AI Governance, Warfighter Trust, AI Product and Acquisition Life Cycle, Requirements Validation, Responsible AI Ecosystem, and AI Workforce.

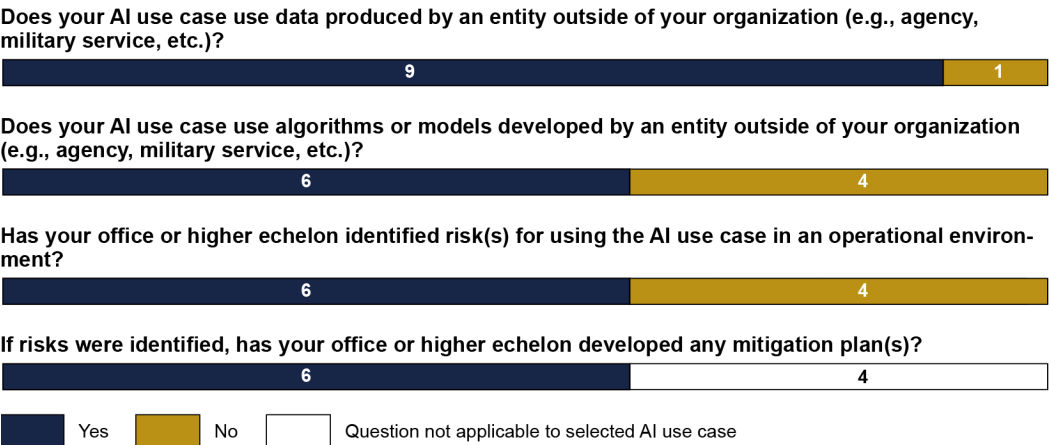
Figure 16: Survey Response Frequencies from 10 Selected Department of Defense Officials Regarding Responsible Artificial Intelligence (AI) Tenet 2, Warfighter Trust



Source: GAO analysis of survey information. | GAO-27-107837

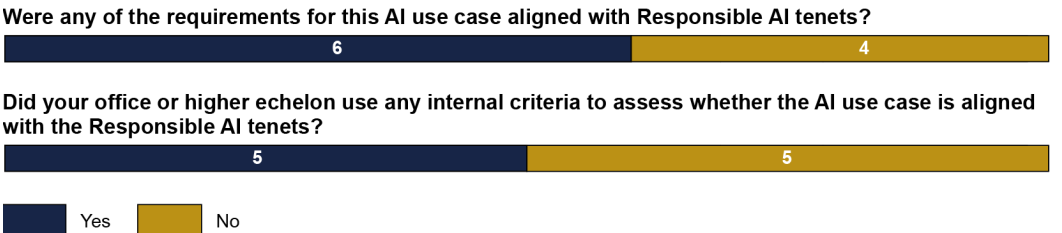
Note: The one use case that reported no test, evaluation, verification, and validation mechanisms stated that it would do so during a later development phase.

Figure 17: Survey Response Frequencies from 10 Selected Department of Defense Officials Regarding Responsible AI Tenet 3, Artificial Intelligence (AI) Products & Acquisition Life Cycle



Source: GAO analysis of survey information. | GAO-27-107837

Figure 18: Survey Response Frequencies from 10 Selected Department of Defense Officials Regarding Responsible Artificial Intelligence (AI) Tenet 4, Requirements Validation



Source: GAO analysis of survey information. | GAO-27-107837

Table 3: (U) Survey Response Frequencies from 10 Selected Department of Defense Officials Regarding Improvements That Could Help Implement Responsible Artificial Intelligence (AI)

Which of the following, if any, would increase your office's or organization's ability to incorporate the six Responsible AI tenets into your AI use case?	Number of components
Access to additional Responsible AI staff or expertise	7
Sharing of Responsible AI resources and/or best practices	6
Adding the Chief Digital and Artificial Intelligence Officer's Responsible AI tools, or access to Responsible AI tools, on classified domains	6
Additional training for AI or Machine Learning developers	6
Support in developing requirements that align with Responsible AI tenets	5
Clearer governance roles and responsibilities for overseeing Responsible AI implementation	5
Internal process improvements	5
A better understanding of how to embed Responsible AI tenets into Testing Evaluation Verification, and Validation processes	4
Detailed guidance on how to implement Responsible AI tenets	4
Greater transparency in data, algorithm, or model characteristics developed by external organizations	4
Additional training for AI or Machine Learning users	4
Periodic assessments of how well an AI or Machine Learning project aligns with Responsible AI tenets	3

Source: GAO analysis of survey information. | GAO-27-107837

Note: These responses were offered to respondents to select if applicable to their use case. The above responses were to the question “Which of the following, if any, would increase your office’s or organization’s ability to incorporate the six Responsible AI tenets into your AI/ML capability”. An open-ended follow up question for these responses asked “If you checked “yes” for any of the rows above, or have other recommendations not listed, please elaborate on those here. Respondents used this space to share challenges and potential promising practices.

In addition to the quantitative analysis in this appendix, our report included qualitative analysis of the survey results in the section “What are some of the reported and potential benefits of collaboration?” The responses to the below survey questions were used in that qualitative analysis.

1. Did development of the AI/ML capability involve any coordination or collaboration on Responsible AI tenets with other DOD organizations, including defense intelligence elements? Please note that we will be asking separately about coordination or collaboration with the Intelligence Community outside of DOD below. Please check one. Response choices were “Yes” or “No.”
 - a. If yes, what type(s) of outcomes, positive or negative, were observed from this collaboration/coordination (e.g., knowledge sharing, promoting norms, slowing down progress, increasing cost)? Open ended response.

2. Did development of the AI/ML capability involve any coordination or collaboration on Responsible AI tenets with the Intelligence Community (outside of DOD)? Please check one. Response choices were “Yes” or “No.”

- a. If yes, what type(s) of outcomes, positive or negative, were observed from this collaboration/coordination (e.g., knowledge sharing, promoting norms, slowing down progress, increasing cost?). Open ended response

3. Did development of the AI/ML capability involve any coordination or collaboration on Responsible AI tenets with Industry? Please check one. Response choices were “Yes” or “No.”

- a. If yes, what type(s) of outcomes, positive or negative, were observed from this collaboration/coordination (e.g., knowledge sharing, promoting norms, slowing down progress, increasing cost?). Open ended response

4. Did development of the AI/ML capability involve any coordination or collaboration on Responsible AI tenets with any other entities (e.g., other U.S. government agencies, international entities, academia, FFRDCs, etc.)? Please check one. Response choices were “Yes” or “No.”

- a. If yes, what other entities were collaborated with or coordinated with? Open ended response.
- b. What type(s) of outcomes, positive or negative, were observed from this collaboration/coordination (e.g., knowledge sharing, promoting norms, slowing down progress, increasing cost?). Open ended response

Appendix III: Survey Methodology

We conducted a nongeneralizable survey of 10 Department of Defense (DOD) components to understand how they have implemented Responsible Artificial Intelligence (AI) tenets as described in DOD’s 2022 *Responsible AI Strategy and Implementation Pathway (Pathway)* in 10 selected AI use cases (one per component). We selected 10 DOD components that included major defense agencies and the five military services. We identified potential use cases from these components by reviewing a January 2025 Office of the Chief Digital and AI Officer (CDAO) inventory list of 378 AI use cases and then working with CDAO subject matter experts to refine a subset of the list using parameters we selected, as described in “How GAO Did This Study” above. The selected use cases came from the Army, Navy, Air Force, Space Force, Marine Corps, Defense Intelligence Agency, National Geospatial-Intelligence Agency, Defense Threat Reduction Agency, U.S. Special Operations Command, and U.S. Cyber Command. We asked the components to identify cognizant officials working on each selected AI use case who could answer survey questions, or collect responses from cognizant subject matter experts working on the use case, about how they were implementing DOD’s responsible AI tenets in their use case.

The survey included general questions about the use case as well as questions about how, if at all, the organization responsible for the use case incorporated each of the tenets for that use case. The questionnaire was organized by the tenets in the 2021 Deputy Secretary of Defense memorandum *Implementing Responsible AI in the Department of Defense*, but specific implementation questions were based on additional information in DOD’s *Pathway* and other relevant sources.³³ Appendix II includes the questions we asked in the survey whose responses were used in our analysis.

The draft questionnaire was developed with a GAO survey specialist. One subject matter expert in the DOD CDAO reviewed the draft questionnaire for substantive issues and a second GAO survey specialist reviewed the questionnaire for technical issues, and we modified the questionnaire as needed. To minimize errors that might occur from respondents interpreting our questions differently than we intended, we pretested our questionnaire using cognitive interviewing techniques with knowledgeable officials familiar with the use cases. We noted any potential problems and modified the questionnaire based on the pretest results.

We fielded the survey from June 12, 2025, through August 14, 2025, to cognizant use case officials. We emailed the questionnaire as a Microsoft Word form. Respondents could complete and return unclassified responses or responses up to Top Secret. The survey response rate was 100 percent. Nine organizations returned unclassified/Controlled Unclassified Information (CUI) survey responses, and one organization submitted Secret-level survey responses. That organization stated that its survey responses were unclassified if anonymized and reported in aggregate. After reviewing survey responses, we conducted additional follow-up, as appropriate, with each component to get clarifying and current information on each use case.

To conduct our analysis, survey responses were manually entered into Microsoft Excel by one analyst and the data entry was verified by a second analyst. We analyzed closed-ended (e.g., Yes/No) questions by tallying the responses to each question and those computations were verified by a second analyst. To assess whether the selected component use cases had taken steps to implement each tenet, we analyzed closed and open-ended responses to key survey questions using a standard coding scheme with two implementation levels: Step(s) Taken- the use case survey response described action(s) taken to incorporate one or more aspects of the Responsible AI tenet; No Steps Taken- the use case survey response did not describe any actions to incorporate any aspects of the Responsible AI tenet. Two analysts independently conducted analyses and any initial disagreements in the coding were discussed and reconciled by the analysts.

The survey results are meant to be a summary of the experiences of 10 use cases and are not generalizable to any other use cases.

Endnotes

¹Department of Defense, *Responsible Artificial Intelligence Strategy and Implementation Pathway* (June 2022).

²According to the Federal Chief Information Officers Council, an AI use case refers to the specific scenario in which AI is designed, developed, procured, or used to advance the execution of agencies' missions and their delivery of programs and services, enhance decision-making, or provide the public with a particular benefit.

³We conducted a nongeneralizable survey of 10 DOD components to understand how they have been implementing Responsible AI tenets in the *Pathway*. For more information on selected use cases, see "How GAO Did This Study."

⁴CDAO officials said that there are probably more than 378 use cases across the department; they reported 378 based on data available to them at that time. As of February 2026, the officials were attempting to collect more data to report an updated number of use cases.

⁵Department of Defense, *Responsible Artificial Intelligence Strategy and Implementation Pathway* (June 2022).

⁶Department of Defense, Secretary of Defense Memorandum, *Artificial Intelligence Ethical Principles for the Department of Defense* (Feb. 21, 2020).

⁷Department of Defense, Deputy Secretary of Defense Memorandum, *Implementing Responsible Artificial Intelligence in the Department of Defense* (May 26, 2021).

⁸Department of Defense (DOD) Directive 5105.89, *Chief Digital and Artificial Intelligence Officer* (Nov. 18, 2024).

⁹According to DOD Directive 5105.89, the CDAO may also establish DOD policy within its area of assigned responsibilities and functions and assign responsibilities to DOD components.

¹⁰Department of Defense, *Data, Analytics, and Artificial Intelligence Adoption Strategy* (Nov. 2, 2023).

¹¹Department of Defense, Deputy Secretary of Defense Memorandum, *Realigning the Office of the Chief Digital and Artificial Intelligence Officer to Accelerate Department-wide Artificial Intelligence Transformation* (Aug. 14, 2025). The Congressional Research Service issued an updated report on this realignment in December 2025, noting that this realignment is an effective demotion for CDAO within the department. See Congressional Research Service, *Realignment of DOD's Chief Digital and AI Officer (CDAO)* (Dec. 1, 2025).

¹²Department of Defense, Deputy Secretary of Defense Memorandum, *Establishment of the Chief Digital and Artificial Intelligence Officer* (Dec. 8, 2011).

¹³In addition to CDAO integrating and then succeeding the Joint Artificial Intelligence Center, in February 2022 additional organizations were realigned to CDAO. Specifically, CDAO gained authority, direction, and control over the resources and personnel associated with the Office of the Under Secretary of Defense (Comptroller) Office of Advancing Analytics (ADVANA). Further, the DOD Chief Data Officer was operationally realigned to the Office of the CDAO.

¹⁴The William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021, Pub. L. No. 116–283 § 232, (2021), which provided that during 2 years beginning on the date of the enactment (Jan. 1, 2021), the Director of the Joint Artificial Intelligence Center shall report directly to the Deputy Secretary of Defense without intervening authority.

¹⁵The federal minimum risk management practices for high impact AI are outlined in Office of Management and Budget Memorandum M-25-21, *Accelerating Federal Use of AI through Innovation, Governance, and Public Trust* (Apr. 3, 2025).

¹⁶Chief AI Officers Council AI Assurance Working Group, *Chief AI Officer AI Minimum Risk Management Resources, v.1.0* (September 2025).

¹⁷Department of Defense, Chief Digital and Artificial Intelligence Officer, *Guidelines and Guardrails to Inform Governance of Generative Artificial Intelligence* (July 12, 2024).

¹⁸We assessed whether a use case had taken steps to incorporate a tenet based on the definitions of the tenets and the information provided in the survey responses. As noted later in our report, DOD has not established measures to assess the implementation of Responsible AI.

¹⁹Defense Intelligence Agency, *Quality Assurance Framework Instruction Manual* (n.d.).

²⁰CDAO officials noted that one of the lines of effort in the *Pathway* called for component Responsible AI leads to work through assigned lines of effort and collaborate with others that were assigned alongside their component.

²¹Department of Defense, Chief Digital and Artificial Intelligence Officer, *Guidelines and Guardrails to Inform Governance of Generative Artificial Intelligence* (Jul. 12, 2024).

²²Department of Defense, *Data, Analytics, and Artificial Intelligence Adoption Strategy*, (Nov. 2, 2023); Department of Defense, *Responsible Artificial Intelligence Strategy and Implementation Pathway* (June 2022).

²³GAO, *Artificial Intelligence: DOD Should Improve Strategies, Inventory Process, and Collaboration Guidance*, GAO-22-105834 (Washington, D.C.: Mar. 30, 2022).

²⁴U.S. Special Operations Command reported collaboration with industry or other U.S. government agencies, international entities, academia, and Federally Funded Research and Development Centers on capabilities with operational needs. Army's Project Linchpin and Army Research Laboratory reported collaboration on adoption of Responsible AI principles in their use case

development that enabled project success. Navy officials reported trying to maximize collaborative activities like knowledge sharing, architecture alignment, contracting opportunities, and risk reduction for all Responsible AI with Office of Secretary of Defense, Defense Innovation Unit, Chief Digital and AI Office, other service components, intelligence community, Federally Funded Research and Development Centers, University Affiliated Research Centers, and industry partners. Space Force officials reported that industry was very receptive to collaborative discussions and had generally positive outcomes from knowledge sharing with industry and the Massachusetts Institute of Technology Lincoln Lab, Air Force Research Lab, Army, and National Reconnaissance Office.

²⁵See appendix II for details on the related survey question and responses.

²⁶See appendix II for details on the related survey question and responses.

²⁷CDAO Responsible AI officials told us that they have developed a number of metrics related to the Responsible AI tools that measure the experiences of individuals and offices using the Responsible AI tools. Examples of these metrics include number of unique visitors on the toolkit webpage, visit duration, and number of actions taken, such as downloading materials. It was unclear from survey responses whether DOD components have found CDAO's Responsible AI tools helpful in addressing implementation challenges. Among the 10 components we surveyed, two used CDAO's Responsible AI tools for the selected use case we asked them about, seven did not use it, and one did not know if it had used it.

²⁸GAO, *Artificial Intelligence: Actions Needed to Improve DOD's Workforce Management*, GAO-24-105645 (Washington, D.C.: Dec. 14, 2023).

²⁹Deputy Secretary of Defense Memorandum, *Implementing Responsible Artificial Intelligence in the Department of Defense* (May 26, 2021).

³⁰Deputy Secretary of Defense Memorandum, *Establishment of the Chief Digital and Artificial Intelligence Officer* (Dec. 8, 2021).

³¹Deputy Secretary of Defense Memorandum, *Realigning the Office of the Chief Digital and Artificial Intelligence Officer to Accelerate Department-wide Artificial Intelligence Transformation* (Aug. 14, 2025).

³²Department of Defense, *Responsible Artificial Intelligence Strategy and Implementation Pathway* (2022).

³³Deputy Secretary of Defense Memorandum, *Implementing Responsible Artificial Intelligence in the Department of Defense* (May 26, 2021). Other relevant sources included Department of Defense, *Responsible Artificial Intelligence Strategy and Implementation Pathway* (2022).