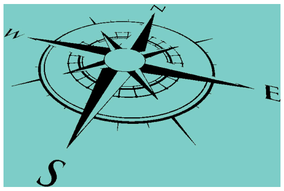
Audit of Governance and Protection of Department of Defense Artificial Intelligence Data and Technology -- Recommendations

The original objective of this audit was to determine whether the DoD's artificial intelligence (AI) portfolio had gaps and weaknesses related to the governance, protection, and ownership rights of AI data and technologies. However, when we initiated the audit, we determined that the DoD had not yet developed an enterprise-wide AI governance framework or standards and that AI projects were being developed and coordinated by the individual DoD Components. Therefore, we revised our objective to determine the DoD's progress in developing an AI governance framework and standards, and to determine whether the DoD Components implemented security mechanisms to protect AI data and technologies from internal and external cyber threats.

Contents



Office of the Inspector General U.S. Department of Defense (DODOIG)

Stakeholder(s):

Carol N. Gorman :
Assistant Inspector General for Audit, Cyberspace Operations

Vision

Secure, well-governed AI technologies

Mission

To determine the DoD’s progress in developing an Artificial Intelligence (AI) governance framework and standards and to determine whether the DoD Components implemented security controls to protect AI data and technologies from internal and external cyber threats.

Values

Collaboration

Knowledge

Transparency

Capabilities

Privacy

Security

Civil Liberties

1. AI Governance

Establish an AI governance framework.

Stakeholder(s)

JAIC Director :
Joint Artificial Intelligence Center

We recommend that the JAIC Director establish an AI governance framework that, among other things, includes a standard definition of AI; a central repository for AI projects; a security classification guide; and a strategy for identifying similar AI projects and for promoting the collaboration of AI efforts across the DoD.

1.1. Definition

Include a standard definition of Artificial Intelligence.

The FY 2019 NDAA directed the Secretary of Defense to establish a standard definition for AI by August 2019, but as of March 2020, a standard definition of AI within the DoD did not exist. Broadly defined in industry, AI is a branch of computer science dealing with the simulation of intelligent behavior in computers.

Stakeholder(s):

Army :
Component's Definition of Artificial Intelligence: An automated system that can learn on its own and perform multiple tasks using machine learning. ~ Army AI Task Force

Navy :
Component's Definition of Artificial Intelligence: The theory and development of computer systems able to perform tasks normally requiring human intelligence, such as visual perception, speech recognition, decision-making, and translation between languages. ~ AI Portfolio Lead

Air Force :
Component's Definition of Artificial Intelligence: AI refers to the ability of machines to perform tasks that normally require human intelligence… whether digitally or as the smart software behind autonomous physical systems. ~ 2019 United States Air Force Artificial Intelligence Annex

DTRA :
Component's Definition of Artificial Intelligence: The science/goal to develop computational systems that can reason about problems and solve them without being explicitly programmed to perform the task and that adapt to new situation based on exposure to previous information. ~ Data Science AI Office*

SCO :
Component's Definition of Artificial Intelligence: The rapid use of broad information to inform analytic decision making. ~ Portfolio Leader for Autonomy and AI

Defense Innovation Board :
The Defense Innovation Board conducted a project on AI ethics principles, and defined AI as "a variety of information processing techniques and technologies used to perform a goal-oriented task and the means to reason in the pursuit of that task."

Air Force Research Laboratory :
... individuals within the same DoD Component defined AI differently. For example, a technical manager at the Air Force Research Laboratory identified a missile project as an AI project because the project used autonomous technology and algorithms. However, the project manager of the same project said that the project was an autonomy project that uses predefined flight formations and was not an AI project.

Office of Naval Research :
In addition, an Office of Naval Research contractor identified an unmanned vehicle project as an AI project, but the AI Portfolio lead for the Office of Naval Research stated that he considered the project an autonomy project that uses AI technology to identify sensor images, and not an AI project.

RAND :
While some definitions were similar, the varying AI definitions present a challenge to DoD Components in determining what is considered an AI project, since many projects use some level of AI. RAND concluded that a definition would not help the DoD identify its AI investments or assess its AI talent needs because of the rapid pace of technological change and the challenges in anticipating the rate and use of technological advances. However, we believe a standard definition is necessary.

JAIC :
The JAIC needs to develop a standard definition of AI.

1.1.1. Investments

Account for and govern its AI investments.

At a minimum, a standard definition would help the DoD account for and subsequently govern its AI investments.

1.1.2. Goals

Consider DoD's goals for using AI and evolve them as AI changes.

The definition should consider the DoD's goals for using AI and should evolve as AI changes.

1.1.3. Oversight

Apply oversight and governance consistently across the DoD.

Without a clear and standard AI definition, the DoD's AI oversight and governance could be applied inconsistently across the DoD.

1.2. Security Classification

Include a security classification guide.

Security Classification Guidance — The JAIC needs to develop a security classification guide to help DoD Components identify sensitive and classified information, and apply the appropriate security markings to ensure that information used to support AI projects are properly protected.

1.2.1. Information Elements

Identify elements of information that require security protection.

It is essential for the JAIC to identify specific elements of information that require security protection to prevent adversaries from applying effective countermeasures to the AI capability.

1.2.2. Accuracy

Enable accurate classification of AI information and help improve derivative classification decisions for AI information.

DoD Manual 5200.45, "Instructions for Developing Security Classification Guides," requires the Military Services and DoD Components to issue timely and comprehensive guidance on the classification of information, which, if disclosed to an unauthorized person, could cause damage to national security. A properly constructed classification guide will enable accurate classification of AI information and help improve derivative classification decisions for AI information... security protections, if warranted, as defined by DoD Manual 5200. 45. This type of information could also be used in AI projects.

1.2.3. Component Failures

Use performance information from key equipment sensors and components to anticipate component failures.

For example, when applying predictive maintenance, the AI technology can use performance information from key equipment sensors and components to anticipate component failures and reduce the amount of unplanned maintenance...

1.2.4. Capabilities & Vulnerabilities

Identify information that may disclose present or future strategic or tactical capabilities and vulnerabilities.

Given that many types of data support AI projects, the JAIC should work in conjunction with the DoD Components to identify information that may disclose present or future strategic or tactical capabilities and vulnerabilities. Avoiding the unauthorized or inadvertent disclosure of critical DoD information requires the implementation of a comprehensive security classification guide for the data and technology that support AI projects.

1.3. Strategy

Develop a strategy to identifying similar AI projects and promote the collaboration of AI efforts across DoD.

Maintaining Accountability of and Collaborating on Artificial Intelligence Projects

1.3.1. Projects

Accurately track AI projects.

The JAIC needs to develop a process to accurately track AI projects. An AI inventory management process for identifying and developing a baseline of AI projects is necessary to maintain awareness of the types and number of AI projects across the DoD. In April 2019, we conducted a data call requesting a list of AI projects from 23 DoD Components and compared our results to the list of AI projects provided by Cost Assessment and Program Evaluation (CAPE), who initiated a data call for AI projects in April 2018. We determined that CAPE's list included AI projects that were no longer ongoing.

1.3.2. Investment Reviews

Conduct annual or biannual reviews of the DoD's AI investments.

The RAND report acknowledges that the JAIC needs to maintain visibility of DoD AI activity, which includes accounting for DoD AI programs and projects. To maintain visibility of DoD AI activity, the report recommended that the JAIC conduct annual or biannual reviews of the DoD's AI investments. Based on the comparison of the CAPE list and our data call results, we agree with the RAND report that the JAIC should require DoD Components to report their AI projects on a prescribed basis. Maintaining visibility of DoD AI activity should include a monitoring process for identifying and validating the status of AI projects; developing a baseline of AI projects; and reporting AI projects to the JAIC continually. Without a reliable baseline of active AI projects within the DoD and continual monitoring of planned and active AI projects, the JAIC will not be able to effectively execute its mission to maintain an accounting of DoD AI initiatives as a means of synchronizing efforts and fostering collaborations across the DoD.

1.3.3. Collaboration

Ensure the DoD Components collaborate among themselves.

In addition to developing a process for tracking AI projects, the JAIC needs to develop a process to ensure the DoD Components collaborate among themselves, which would promote joint opportunities for developers and users of AI to consolidate resources and save money. Collaboration between and within the DoD Components provides the opportunity to support informed decision making, share situational awareness, and improve knowledge. A collaboration strategy should consider a process for assessing mission needs, collecting and analyzing data to determine relevant patterns or trends, integrating knowledge related to mission needs, and sharing information that will benefit the DoD Components.

1.3.3.1. Needs

Assess mission needs.

1.3.3.2. Patterns & Trends

Collect and analyze data to determine relevant patterns or trends.

1.3.3.3. Knowledge

Integrate knowledge related to mission needs.

1.3.3.4. Information Sharing

Share information that will benefit the DoD Components.

1.3.4. Transparency & Savings

Jointly develop AI projects that would promote transparency and save resources.

A collaboration process could result in jointly developed AI projects that would promote transparency and save resources. For example, the Marine Corps is developing a technology that will use multiple indicators to identify marines who could be at risk of suicide, and according to a Marine Corps chief analyst, the Army is using data analytics to assist in suicide prevention. The Army could work with the Marine Corps to develop a joint AI technology that might be suitable for any Military Service to collect relevant data that can be used to identify those most likely to commit suicide, so that treatment could be initiated in a timely manner. The RAND report recommended that the JAIC host a workshop with AI technical leaders to discuss AI activities across the DoD. The workshop would allow AI technical leaders to collaborate on AI activities and would promote information exchange between DoD Components. Based on our audit work, we agree with the RAND report that DoD AI leaders should collaborate on AI activities and exchange information on AI projects, and lessons learned. Collaboration between DoD Components will improve the efficiency of operations, enhance situational awareness, and contribute to missions that are more successful.

1.4. Project Repository

Develop a repository that will allow DoD Components to store and share data and tools used to support AI projects.

Artificial Intelligence Data and Tool Repository — The JAIC needs to develop a central repository that will allow DoD Components to store and share data and tools used to support AI projects.

1.4.1. Capabilities

Enable the rapid delivery of AI-enabled capabilities.

A central repository will enable the rapid delivery of AI-enabled capabilities and allow AI developers to quickly access the data and tools needed to build the AI technology. Sharing tools would also reduce the DoD's acquisition costs by reducing the overall expense of individual AI projects. The DoD AI Strategy directs the JAIC to develop a central repository of shared data and reusable tools.

Stakeholder(s):

JAIC :

As of March 2020, the JAIC had not taken steps to develop a central repository and did not provide a timeline for when it expects to develop one. However, officials from the Navy, Marine Corps, and the SCO stated that the DoD would benefit from such a repository.

Marine Corps :

For example, a chief analyst for the Marine Corps stated that a central location to store AI data would eliminate the burden of sharing information across the DoD, thereby improving access to data that Components could use to support AI projects.

Navy :

A Navy AI program manager also stated that the implementation of the central repository would help with the secure sharing of AI data across the DoD.

RAND :

The RAND report cited the lack of access to data and the ability to share data as an inhibitor to innovation. In addition, the RAND report stated that DoD officials expressed concern with finding solutions and learning from the successful efforts of others, and a desire for an environment for sharing tools, tips, and best practices. According to the report, interviewees expressed the need for shared resources that would help remove barriers to accessing data. A central repository for sharing data used to support AI projects could also reduce the amount of duplicate data stored on DoD networks.

DoD Data Centers :

Furthermore, the Data Center Optimization Initiative, designed to reduce the DoD's data center footprint, encourages transitioning to a central repository for data storage, which could also help the DoD more efficiently store its data. An option for developing a central repository could be the use of a cloud environment. According to the DoD Cloud Strategy, a cloud provides the ability to scale and secure both the collection and the analysis of data stored in an enterprise DoD cloud. The cloud strategy gives mission owners the ability to make decisions with the most relevant information and allows for a more flexible execution environment while simultaneously providing increased information security. A cloud environment also allows for a high volume of data storage without sacrificing workstation performance.

1.4.2. Data & Tools

Allow AI developers to quickly access the data and tools needed to build the AI technology.

Stakeholder(s):

AI Developers

1.5. Legality & Privacy Standards

Issue standards for assessing legal and privacy considerations when developing and using AI data and technologies.

Legal and Privacy Standards for Artificial Intelligence Projects — The JAIC needs to issue standards for assessing legal and privacy considerations when developing and using AI data and technologies.

1.5.1. Laws & Liberties

Assess the legal implications of using AI in an operational environment to prevent violations of current laws and civil liberties.

Standards related to legal considerations are needed to ensure DoD Components and DoD contractors assess the legal implications of using AI in an operational environment to prevent violations of current laws and civil liberties. For example, AI-controlled vehicles are designed to identify people and other vehicles, and make decisions such as allowable speed and direction of travel. However, if the AI-controlled vehicle is unable to accurately identify an object and makes a decision that turns deadly, a determination of legal responsibility is needed. However, as stated in the RAND report, the standards should not be too restrictive, as DoD officials have expressed concerns that applying too many regulations on using AI could stifle innovation.

Stakeholder(s):

DoD Components

DoD Contractors

1.5.2. Privacy

Comply with privacy laws when using personal information during the development and use of AI technologies.

DoD privacy standards are also needed to ensure that DoD Components comply with existing privacy laws when using personal information during the development and use of AI technologies. The Privacy Act of 1974 establishes certain controls over the type of personal information the Federal Government can collect and use. As the DoD experiments with emerging technologies such as AI, it must ensure that DoD Components comply with existing privacy laws when developing and using AI data and technologies... Although Federal and DoD standards may apply to AI, the DoD should either supplement existing privacy standards or create new standards specific to AI. The privacy standards should include guidance for collecting personal information and obtaining consent to use the data to support AI projects. The standards would help DoD Components make informed decisions about the data's relevance to the AI project as well as help prevent the misuse of the data.

Stakeholder(s):

National Institute of Standards and Technology :

According to the National Institute of Standards and Technology, privacy considerations should be included in any standards governing the collection, processing, sharing, storage, and disposal of personal information.

2. Security Controls

Develop and implement a plan to correct the security control weaknesses among the military services

Stakeholder(s)

Army CIO

Marine Corps CIO

Navy CIO

Air Force CIO

We also recommend that the Army, Marine Corps, Navy, and Air Force CIOs develop and implement a plan to correct the security control weaknesses related to using strong passwords; monitoring networks and systems for unusual activity; locking systems after inactivity, and implementing physical security controls.

2.1. Passwords

Correct the security control weaknesses related to using strong passwords.

2.2. Monitoring

Correct the security control weaknesses related to monitoring networks and systems for unusual activity.

2.3. Inactivity Locking

Correct the security control weaknesses related to locking systems after inactivity.

2.4. Physical Security

Correct the security control weaknesses related to implementing physical security controls.

3. Contractors

Develop and implement a plan to verify that contractors correct security control weaknesses.

Stakeholder(s)

DoD Contractors

Defense Threat Reduction Agency (DTRA)

Strategic Capabilities Office (SCO) Security

Lastly, we recommend that the contracting officer for the Defense Threat Reduction Agency (DTRA), and the Strategic Capabilities Office (SCO) Security and Program Protection Director, in coordination with their DoD requiring activities, develop and implement a plan to verify that contractors correct the security control weaknesses identified in this report.

Administrative Information

Start Date: 2020-06-29
End Date:

Publication Date: **2020-07-07**
Source: https://media.defense.gov/2020/Jul/01/2002347967/-1/-1/1/DODIG-2020-098.PDF

Submitter:

Given Name: Owen
Surname: Ambur
Email: Owen.Ambur@verizon.net
Phone: