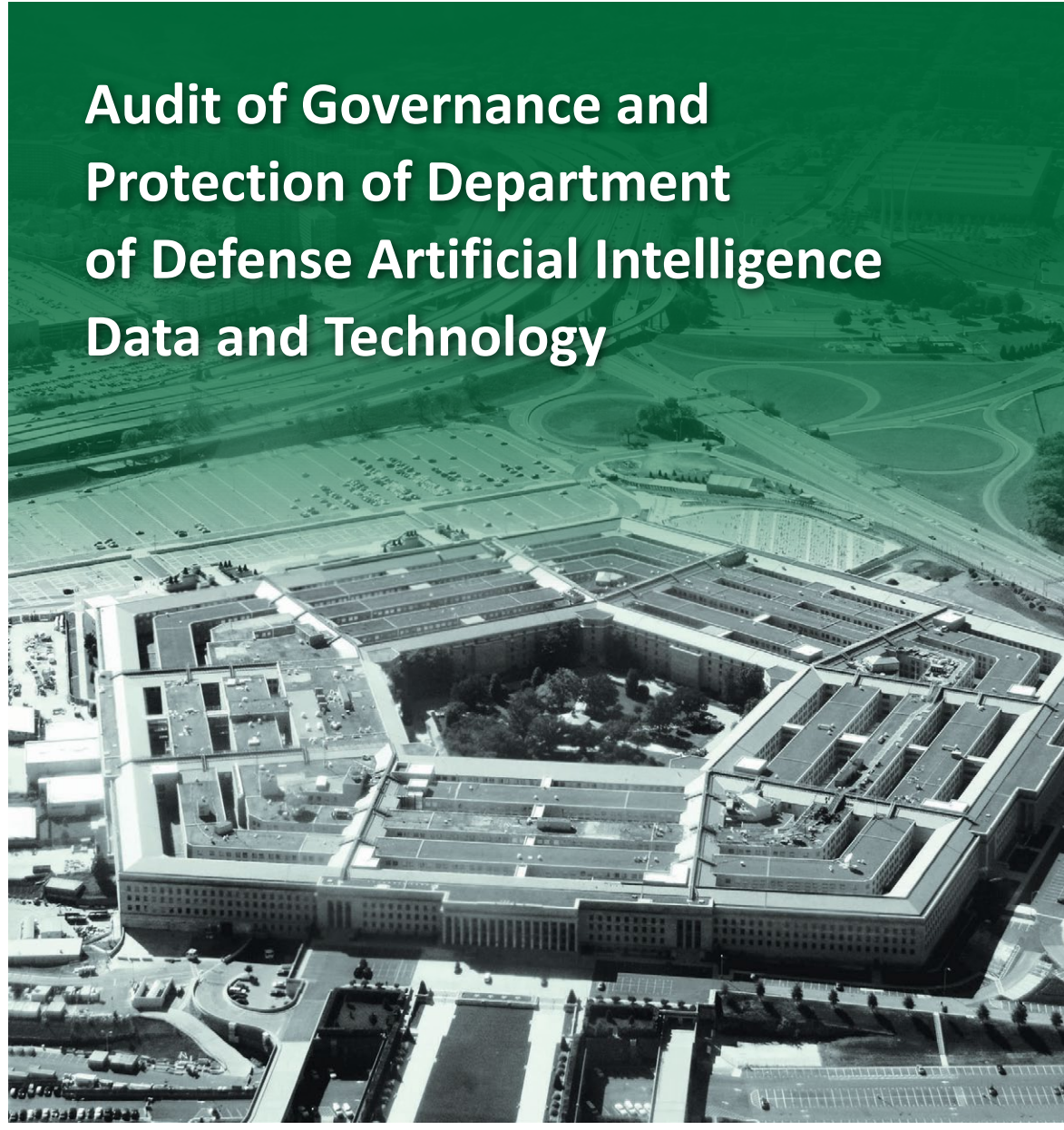


~~FOR OFFICIAL USE ONLY~~

# INSPECTOR GENERAL

*U.S. Department of Defense*

JUNE 29, 2020



## Audit of Governance and Protection of Department of Defense Artificial Intelligence Data and Technology

INTEGRITY ★ INDEPENDENCE ★ EXCELLENCE

The document contains information that may be exempt from mandatory disclosure under the Freedom of Information Act.

~~FOR OFFICIAL USE ONLY~~







# Results in Brief

## *Audit of Governance and Protection of Department of Defense Artificial Intelligence Data and Technology*

June 29, 2020

### Objective

The objective of this audit was 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.

### Background

On August 13, 2018, the FY 2019 National Defense Authorization Act (NDAA) directed the Secretary of Defense to designate a senior official to coordinate DoD efforts to develop, mature, and transition AI technologies into operational use. The FY 2019 NDAA defines AI as "any artificial system that performs tasks under varying and unpredictable circumstances without significant human oversight, or that can learn from experience and improve performance when exposed to data sets."

In June 2018, at the direction of the Deputy Secretary of Defense, the DoD Chief Information Officer (CIO) established the Joint Artificial Intelligence Center (JAIC) to facilitate AI governance, policy, ethics, and cybersecurity. In February 2019, the DoD published its AI Strategy, "Harnessing AI to Advance Our Security and Prosperity," which directed the DoD to accelerate the adoption of AI to transform the future of the battlefield and speed with which the DoD responds to threats.

### Findings

As of March 2020, the JAIC had taken some steps to develop an AI governance framework and standards, such as building the JAIC workforce, developing National Mission objectives, and adopting ethical principles. However, to ensure that the JAIC can meet the responsibilities outlined in the FY 2019 NDAA, DoD AI Strategy, and DoD guidance, the JAIC should also,

- include a standard definition of AI and regularly, at least annually, consider updating the definition;
- develop a security classification guide to ensure the consistent protection of AI data;
- develop a process to accurately account for AI projects;
- develop capabilities for sharing data;
- include standards for legal and privacy considerations; and
- develop a formal strategy for collaboration between the Military Services and DoD Components on similar AI projects.

(FOUO) We also identified that the four DoD Components and two contractors we reviewed did not consistently implement security controls to protect the data used to support AI projects and technologies from internal and external cyber threats. Specifically, the DoD Components and contractors did not consistently,

- configure their systems to enforce the use of strong passwords; generate system activity reports; or lock after periods of inactivity;
- review networks and systems for malicious or unusual activity;
- scan networks for viruses and vulnerabilities; and
- implement physical security controls, such as

[REDACTED] AI data



# Results in Brief

## *Audit of Governance and Protection of Department of Defense Artificial Intelligence Data and Technology*

### **Findings (cont'd)**

Without consistent application of security controls, malicious actors can exploit vulnerabilities on the networks and systems of DoD Components and contractors and steal information related to some of the Nation's most valuable AI technologies. The disclosure of AI information developed by the DoD could threaten the safety of the warfighter by exposing the Nation's most valuable advanced defense technology and causing the United States to be at a disadvantage against its adversaries.

### **Recommendations**

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.

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.

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.

### **Management Comments and Our Response**

The DoD CIO, responding for the JAIC Director, agreed to establish a biannual AI portfolio review with all DoD Components; a central repository for AI projects; legal and privacy standard operating procedures; and

a strategy for collaboration by focusing on early and frequent interaction with users and Service program offices. The DoD CIO's comments were not clear on the actions he will take to develop a standard definition for AI and a security classification guide. Therefore, the JAIC Director should provide additional comments on the final report addressing those recommendations.

(FOUO) The Cybersecurity and Information Assurance Director, responding for the Army CIO; the Deputy Commandant for Information, responding for the Marine Corps CIO; Associate Deputy CIO, responding for the Air Force CIO; and the DTRA Integration Division Director for Research and Development, agreed to develop and implement a plan to correct the security weaknesses we identified. Although the SCO Director, responding for the Security and Program Protection Director, agreed to update policies and conduct quarterly program reviews, he did not agree that

██████████ to security incidents is required. We disagree that ██████████ are not required as they are necessary to ██████████ physical access activities and incidents. Therefore, the Security and Program Protection Director should provide additional comments on the final report addressing that recommendation.

The Deputy Chief of Naval Operations, responding for the Navy CIO, stated that the Navy disagreed with the finding related to physical security. Although the Deputy Chief provided comments on the findings, he did not respond specifically to the recommendations and; therefore, we request that the Navy CIO provide comments on the final report that describe how he plans to address the recommendations.

Please see the Recommendations Table on the next page for the status of recommendations.

## **Recommendations Table**

Management	Recommendations Unresolved	Recommendations Resolved	Recommendations Closed
Chief Information Officer, U.S. Army	None	B.1.a, B.1.b, B.1.c, B.1.d, B.1.e	None
Chief Information Officer, U.S. Marine Corps	None	B.1.a, B.1.b, B.1.e	B.1.c, B.1.d
Chief Information Officer, U.S. Navy	B.1.a, B.1.b, B.1.c, B.1.d, B.1.e	None	None
Chief Information Officer, U.S. Air Force	None	B.1.a, B.1.b, B.1.c, B.1.d, B.1.e	None
Director, Joint Artificial Intelligence Center	A.1.a, A.1.b	A.1.c, A.1.d, A.1.e, A.1.f, A.1.g	None
Contracting Officer, Defense Threat Reduction Agency	None	B.2.a, B.2.c, B.2.e, B.2.g	None
Security and Program Protection Director, Strategic Capabilities Office	B.2.f	B.2.d	B.2.b

Please provide Management Comments by July 29, 2020.

**Note:** The following categories are used to describe agency management’s comments to individual recommendations.

- **Unresolved** – Management has not agreed to implement the recommendation or has not proposed actions that will address the recommendation.
- **Resolved** – Management agreed to implement the recommendation or has proposed actions that will address the underlying finding that generated the recommendation.
- **Closed** – OIG verified that the agreed upon corrective actions were implemented.





**INSPECTOR GENERAL  
DEPARTMENT OF DEFENSE  
4800 MARK CENTER DRIVE  
ALEXANDRIA, VIRGINIA 22350-1500**

June 29, 2020

MEMORANDUM FOR FOR DISTRIBUTION

**SUBJECT:** Audit of Governance and Protection of Department of Defense Artificial Intelligence Data and Technology (Report No. DODIG-2020-098)

This final report provides the results of the DoD Office of Inspector General's audit. We previously provided copies of the draft report and requested written comments on the recommendations. We considered management's comments on the draft when preparing the final report. Those comments are included in the report.

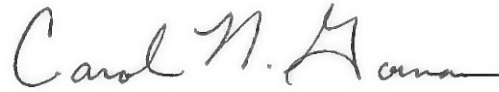
This report contains eight recommendations that are considered unresolved because management officials did not provide written comments on the draft report or did not fully address the recommendations. Therefore, as discussed in the Recommendations, Management Comments, and Our Response sections of this report, the recommendations will remain unresolved until an agreement is reached on the actions to be taken to address the recommendations. Once an agreement is reached, the recommendations will be considered resolved but will remain open until adequate documentation has been submitted showing that the agreed-upon action has been completed. Once we verify that the action is complete, the recommendations will be closed.

This report contains 23 recommendations that are considered resolved. Therefore, as discussed in the Recommendations, Management Comments, and Our Response sections of this report, the recommendations will remain open until adequate documentation has been submitted showing that the agreed-upon action has been completed. Once we verify that the action is complete, the recommendations will be closed.

This report contains three recommendations that are considered closed as discussed in the Recommendations, Management Comments, and Our Response sections of this report. Those recommendations do not require further comments.

DoD Instruction 7650.03 requires that recommendations be resolved promptly. For the unresolved recommendations, please provide us within 30 days your response concerning specific actions in process or alternative corrective actions proposed on the recommendations. For the resolved recommendations, please provide us within 90 days documentation showing that the agreed-upon action has been completed. Your response should be sent as a PDF file to either [audsco@dodig.mil](mailto:audsco@dodig.mil) if unclassified or [REDACTED] if classified SECRET. Responses must have the actual signature of the authorizing official for your organization.

We appreciate the cooperation and assistance received during the audit. Please direct questions to me at [REDACTED]

A handwritten signature in cursive script that reads "Carol N. Gorman".

Carol N. Gorman  
Assistant Inspector General for Audit  
Cyberspace Operations



***Distribution:***

UNDER SECRETARY OF DEFENSE FOR RESEARCH AND ENGINEERING  
UNDER SECRETARY OF DEFENSE FOR ACQUISITION AND SUSTAINMENT  
DIRECTOR, COST ASSESSMENT AND PROGRAM EVALUATION  
CHIEF INFORMATION OFFICER, DEPARTMENT OF DEFENSE  
DEFENSE ADVANCED RESEARCH PROJECTS AGENCY  
AUDITOR GENERAL, DEPARTMENT OF THE NAVY  
AUDITOR GENERAL, DEPARTMENT OF THE ARMY  
AUDITOR GENERAL, DEPARTMENT OF THE AIR FORCE

CC:  
DIRECTOR, STRATEGIC CAPABILITIES OFFICE  
DIRECTOR, DEFENSE INNOVATION UNIT

# Contents

---

## Introduction

Objective.....	1
Background.....	1
Review of Internal Controls.....	4

## Finding A. The JAIC Had Taken Few Steps to Develop an AI Governance Framework and Standards..... 5

The JAIC’s Initial Focus and Progress to Date.....	6
AI Governance Framework and Standards.....	8
Weaknesses in Management of AI Projects Could Threaten Our Military’s Competitive Advantage.....	15
Management Comments on the Finding and Our Response.....	16
Recommendations, Management Comments, and Our Response.....	17

## Finding B. Security Controls for Networks and Systems Supporting AI Projects Were Not Consistently Implemented..... 25

DoD Components and Contractors Did Not Implement Security Controls to Protect AI Data and Technologies.....	26
The DoD’s AI Data and Technologies Could Be Compromised by Cyber Attacks.....	34
Management Comments on the Finding and Our Response.....	34
Recommendations, Management Comments, and Our Response.....	37
Management Comments Required.....	45

## Appendixes

Appendix A. Scope and Methodology.....	52
Use of Computer-Processed Data.....	53
Use of Technical Assistance.....	54
Prior Coverage.....	54
Appendix B. Timeline of JAIC Key Activities.....	56
Appendix C. Sampling Approach.....	58

## Contents (cont'd)

---

### Management Comments

U.S. Army .....	60
U.S. Marine Corps .....	68
U.S. Navy .....	75
U.S. Air Force .....	77
Joint Artificial Intelligence Center .....	79
Defense Threat Reduction Agency .....	83
Strategic Capabilities Office .....	91

<b>Acronyms and Abbreviations</b> .....	94
---	----

<b>Glossary</b> .....	95
-----------------------	----





# Introduction

---

## Objective

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.<sup>1</sup> 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. See Appendix A for a discussion on the scope and methodology and Appendix B for a timeline of Joint Artificial Intelligence Center (JAIC) key activities. Also, see Appendix C for our detailed sampling approach for selecting and assessing the DoD Military Services and Components. See the Glossary for definitions of technical terms.

## Background

On August 13, 2018, the FY 2019 National Defense Authorization Act (NDAA) directed the Secretary of Defense to designate a senior official to coordinate DoD efforts to develop, mature, and transition AI technologies into operational use.<sup>2</sup> The FY 2019 NDAA defines AI as "any artificial system that performs tasks under varying and unpredictable circumstances without significant human oversight, or that can learn from experience and improve performance when exposed to data sets." For example, one of the DoD's AI initiatives is Project Maven, which uses AI to process and identify objects in images and video footage.

In June 2018, the DoD published its AI Strategy, which directed the DoD to accelerate the adoption of AI to transform the future of the battlefield and speed with which the DoD responds to threats.<sup>3</sup> To meet this requirement, the DoD's AI Strategy provides a strategic approach for accelerating AI adoption that focuses on:

- developing AI capabilities that will enhance military situational awareness and decision making;

---

<sup>1</sup> A governance framework includes setting direction, establishing standards, and prioritizing investments.

<sup>2</sup> Public Law 115-232, "The National Defense Authorization Act for Fiscal Year 2019," section 238, "Joint Artificial Intelligence Research, Development, and Transition Activities," August 13, 2018.

<sup>3</sup> Summary of the 2018 Department of Defense Artificial Intelligence Strategy, "Harnessing AI to Advance Our Security and Prosperity," February 12, 2019.

- increasing the safety of operating equipment and streamlining business processes;
- creating a common foundation of shared data and tools and implementing standards to decentralize the development and experimentation of AI;
- building an AI workforce and investing in comprehensive AI training;
- developing strong partnerships with commercial, academic, and international allies to help address global defense challenges; and
- using AI lawfully and ethically to enhance the DoD's key mission areas.

According to the DoD's AI Strategy, AI will impact all of the DoD, including operations, training, sustainment, force protection, recruiting, and health care. By applying AI to defense, the strategy states that the DoD will improve support for and protection of U.S. service members; safeguard our citizens; and defend our allies and partners.

### ***Executive Order on Artificial Intelligence***

In February 2019, the President issued Executive Order 13859, "Maintaining America's Leadership in AI," which states that the U.S. Government should implement an AI Initiative to sustain and enhance the scientific, technological, and economic leadership position of the United States in AI research, development, and deployment.<sup>4</sup> The guiding principles of the AI Initiative include:

- driving technological breakthroughs in AI across the Federal Government, industry, and academia to promote scientific discovery, economic competitiveness, and national security;
- developing appropriate technical standards and reducing barriers to safely testing and deploying AI technologies; and
- promoting an international environment that supports AI industries, while protecting our critical AI technologies from being acquired by competitors and adversarial nations.

In August 2019, in response to the Executive Order, the National Institute of Standards and Technology (NIST) issued a plan for developing technical standards and tools for systems that use AI technologies.<sup>5</sup> The NIST guidance focuses on AI standards for concepts, data, human interactions, metrics, networking, performance testing, safety, risk management, trustworthiness, and security.

---

<sup>4</sup> Exec. Order No. 13859, 84 CFR sec. 3,967 (2019).

<sup>5</sup> National Institute of Standards and Technology, "U.S. Leadership in AI: A Plan for Federal Engagement in Developing Technical Standards and Related Tools," August 9, 2019.

## Joint Artificial Intelligence Center

In June 2018, at the direction of the Deputy Secretary of Defense, the DoD Chief Information Officer (CIO) established the JAIC to facilitate AI governance, standards, ethics, and cybersecurity.<sup>6</sup> In May 2019, the DoD CIO stated that the JAIC would facilitate AI governance, policy, ethics, and cybersecurity by developing a governance framework and standards for AI. The JAIC’s roles and responsibilities, as described in Figure 1, are established by the FY 2019 NDAA, DoD AI Strategy, and Deputy Secretary of Defense.

Figure 1. Joint Artificial Intelligence Center Roles and Responsibilities

FY 2019 NDAA	DoD AI Strategy	Deputy Secretary of Defense
<ul style="list-style-type: none"> <li>• Establish an AI definition for use within the DoD.</li> <li>• Develop a detailed strategic plan to develop, mature, adopt, and transition AI technologies into operational use.</li> <li>• Accelerate the development and fielding of AI.</li> <li>• Develop classification guidance for all DoD AI-related activities.</li> <li>• Develop ethical and legal DoD policies for the development and use of AI.</li> <li>• Develop policy to govern and oversee AI and machine learning.</li> </ul>	<ul style="list-style-type: none"> <li>• Deliver AI-enabled capabilities that address key mission areas, such as improving situational awareness and decision making, increasing the safety of operating equipment, implementing predictive maintenance and supply, and streamlining business processes.</li> <li>• Develop a central repository of AI tools, which will enable decentralized development and experimentation.</li> <li>• Cultivate an AI workforce.</li> <li>• Engage with commercial, academic, and international allies and partners to help address global challenges of significant societal importance.</li> <li>• Lead in military ethics and AI safety.</li> </ul>	<ul style="list-style-type: none"> <li>• Execute National Mission Initiatives.*</li> <li>• Establish a DoD-wide cloud environment that will provide tools, shared data, reusable technologies, processes, and expertise to quickly advance AI across the DoD.</li> <li>• Collaborate within the DoD, across Government, and with industry, academia, and foreign allies to strengthen partnerships, address critical challenges, and advance AI for DoD missions.</li> <li>• Develop a governance framework and standards for AI development and delivery.</li> </ul>

Source: The DoD Office of Inspector General (DoD OIG).

\* National Mission Initiatives (NMIs) are large-scale efforts to apply AI as a solution to closely related and urgent challenges the DoD may encounter.

In October 2019, the Deputy Secretary of Defense formally designated the JAIC Director as the senior official to coordinate the DoD’s AI efforts, in accordance with the FY 2019 NDAA.<sup>7</sup> According to the designation memorandum, by March 2020, the JAIC Director and the Technical Director for Machine Learning and Artificial Intelligence, Office of the Under Secretary of Defense for Research & Engineering

<sup>6</sup> Deputy Secretary of Defense Memorandum, “Establishment of the Joint Artificial Intelligence Center,” June 27, 2018.

<sup>7</sup> Deputy Secretary of Defense Memorandum, “Designation of a Senior Official with Primary Responsibility for Artificial Intelligence,” October 2, 2019.

for AI, must present a formal DoD AI policy, delineate roles and responsibilities as outlined in the FY 2019 NDAA, and develop a formal governance structure that implements Executive Order 13859 and the 2019 DoD AI Strategy. See Appendix B for a timeline of JAIC key activities.

## Review of Internal Controls

DoD Instruction 5010.40 requires DoD organizations to implement a comprehensive system of internal controls that provides reasonable assurance that programs are operating as intended and to evaluate the effectiveness of the controls.<sup>8</sup>

We identified internal control weaknesses related to protecting networks and systems that maintain DoD AI data and technologies. We will provide a copy of the report to the senior officials responsible for internal controls in the Army, Navy, Air Force, JAIC, Defense Threat Reduction Agency, and Strategic Capabilities Office.

---

<sup>8</sup> DoD Instruction 5010.40, "Managers' Internal Control Program Procedures," May 30, 2013.



## Finding A

### The JAIC Had Taken Few Steps to Develop an AI Governance Framework and Standards

As of March 2020, while the JAIC has taken some steps, additional actions are needed to develop and implement an AI governance framework and standards. Although the JAIC was established in June 2018, the JAIC Director was not designated as the senior official to coordinate DoD AI efforts until October 2019. According to JAIC officials, the lack of a formal designation hindered their ability to develop an AI governance framework and standards because they did not have the authority to coordinate AI activities across the DoD. JAIC officials stated that instead of developing an AI governance framework and standards, they focused on building the JAIC workforce, developing National Mission Initiatives, and adopting ethical principles for using AI. The DoD AI Strategy states that a well-designed AI governance framework can help to support and protect U.S. service members and civilians by improving readiness, equipment maintenance, and reducing operational costs. In addition, the effective implementation of AI throughout the DoD can enhance the DoD's ability to predict, identify, and respond to cyber and physical threats.

In December 2018, in response to an FY 2019 NDAA requirement to conduct a study on AI, the JAIC Director, commissioned the RAND Corporation (RAND) to conduct an assessment of the state of AI and recommend actions needed to improve the DoD's AI posture.<sup>9</sup> The RAND report, issued in December 2019, identified critical elements of the DoD's AI posture that the JAIC should address when developing its AI governance framework and standards. We identified some of the same elements during our audit, along with other elements not mentioned in the RAND report. Specifically, when developing its AI governance framework and standards, the JAIC should:

- include a standard definition of AI and regularly, at least annually, consider updating the definition;
- develop a security classification guide to ensure the consistent protection of AI data;
- develop a process to accurately account for AI projects;
- develop capabilities for sharing data;

<sup>9</sup> RAND Corporation, "The Department of Defense Posture for Artificial Intelligence: Assessment and Recommendations," 2019.

- include standards for legal and privacy considerations; and
- develop a formal strategy for collaborating between the Military Services and DoD Components on similar AI projects.

Although those elements are not all-inclusive, including the elements in the governance framework and standards should help ensure that the JAIC can meet the responsibilities outlined in the FY 2019 NDAA, DoD AI Strategy, and Deputy Secretary of Defense memorandums. Developing a comprehensive governance framework during the emergence of AI will help fulfill the DoD's mission to protect the security of our Nation by developing and deploying advanced AI capabilities that ensure the United States sustains its competitive military advantage over its adversaries. An effective governance framework should result in the ability to enforce compliance with decisions about technology use and procurement. In addition, an AI governance framework enables the DoD to develop strong partnerships with commercial, academic, and international allies to help address global defense challenges.

## The JAIC's Initial Focus and Progress to Date

~~(FOUO)~~ As of March 2020, the JAIC had taken some steps to develop an AI governance framework and standards. The FY 2019 NDAA required the JAIC, in coordination with the Secretary of Defense, to develop a definition for AI; a security classification guide; and ethical and legal policies for AI.<sup>10</sup> In addition, the DoD AI Strategy required the JAIC to develop a central repository of AI tools. Furthermore, the Deputy Secretary of Defense required the JAIC to develop a governance framework for developing and delivering AI. However, since its inception in June 2018, the JAIC primarily focused on building its workforce, developing NMIs, and adopting ethical principles for using AI. While JAIC officials acknowledged that the JAIC was behind schedule on delivering a governance framework, they stated that the JAIC did not plan to issue a governance framework until [REDACTED], missing the March 2020 deadline prescribed in the designation memorandum. JAIC officials stated that the AI governance requirements were the responsibility of the designated senior official. The JAIC Director was not appointed as the designated senior official until October 2019.

Before the JAIC Director was designated as the senior official for AI, the JAIC worked with several DoD Components to build the JAIC workforce to include permanent staff. When the Deputy Secretary of Defense established the JAIC, he identified that the JAIC would need to fill at least 27 positions. Initially, the 27 positions were filled with personnel who were detailed to the JAIC for up to

<sup>10</sup> A security classification guide is the written record of an original classification decision or series of decisions regarding a system, plan, program, project, or mission.

6 months. However, the JAIC Deputy Director stated that the JAIC would have difficulty meeting its mission requirements because of the constant turnover of the detailed staff. Therefore, the JAIC focused on hiring permanent staff to fill the 27 positions.

In addition, the JAIC planned on delivering AI capabilities to the DoD through NMIs, which are projects designed to help DoD Components apply AI to life and safety events. For example, the JAIC established the Humanitarian Assistance and Disaster Relief NMI that would improve the DoD's ability to save lives and mitigate the damaging effects of disasters and humanitarian crises. The JAIC also established a Predictive Maintenance NMI, which provides predictive analytics to determine the remaining useful life of a component or subsystem. According to the JAIC, developing NMIs first would help improve military operations by using AI to support and protect U.S. service members, American citizens, and U.S. allies.

In July 2018, DoD leadership requested that the Defense Innovation Board examine AI ethics and develop a set of principles to guide the ethical development and application of AI within the DoD. In October 2019, the Defense Innovation Board released a report on the principles for governing how the DoD develops and uses AI.<sup>11</sup> The report provides recommendations to facilitate the DoD's adoption of ethical principles to promote AI safety and security. The principles discuss the DoD's goals for using AI, such as:

- ensuring human beings exercise the appropriate levels of judgment when developing, deploying, and using AI;
- taking steps to avoid unintended bias that could inadvertently cause harm to individuals; and
- conducting tests on the safety and security of AI systems throughout the systems' life cycles.

The Defense Innovation Board issued 12 recommendations to aid the DoD in implementing the ethical principles. Among other recommendations, the Defense Innovation Board recommended that the DoD:

- establish a DoD-wide AI steering committee that ensures the DoD's AI projects are consistent with the DoD AI ethical principles;
- create a taxonomy of DoD uses of AI based on ethical, safety, and legal risk considerations; and
- assess the appropriate implementation of the AI ethical principles.

On February 24, 2020, the DoD adopted the ethical principles recommended by the Defense Innovation Board.

<sup>11</sup> Defense Innovation Board, "AI Principles: Recommendations on the Ethical Use of Artificial Intelligence by the Department of Defense," October 2019.

## AI Governance Framework and Standards

To determine what elements should be considered in developing an AI governance framework, we interviewed key personnel responsible for governing and overseeing the development and implementation of AI technologies. These key personnel included officials from the Army, Navy, Air Force, Marine Corps, Defense Threat Reduction Agency (DTRA), and the Strategic Capabilities Office (SCO). In addition, we analyzed the RAND report to identify similar elements that we identified during the audit and recommended actions for developing an AI governance framework. Based on our interviews and analyses, we identified the following elements that should be considered in developing an AI governance framework:

- A standard definition of AI.
- A security classification guide.
- A process to accurately account for AI projects.
- Capabilities for sharing data.
- Standards for legal and privacy considerations.
- A formal strategy for collaborating between the Military Services and DoD Components on similar AI projects.

Four of these six elements were also identified in the RAND report as critical to addressing AI challenges. Although not all-inclusive, these elements would help ensure that the JAIC can meet the responsibilities outlined in existing guidance.

### ***Definition of Artificial Intelligence***

The JAIC needs to develop a standard definition of AI. 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. We asked each of the DoD Components that we visited to provide us with its definition of AI (see Table 1).



Table 1. Examples of DoD Component Definitions of Artificial Intelligence

Component	Component's Definition of Artificial Intelligence
Army	An automated system that can learn on its own and perform multiple tasks using machine learning. – Army AI Task Force
Navy	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	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	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	The rapid use of broad information to inform analytic decision making. – Portfolio Leader for Autonomy and AI

Source: The DoD OIG.

\* This definition has not been formally approved.

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.”<sup>12</sup> As shown in Table 1, each Component had a different definition of AI, which resulted in AI projects being inconsistently identified. In addition, 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.<sup>13</sup>

<sup>12</sup> The Defense Innovation Board is an independent federal advisory committee that provides advice and recommendations to DoD senior leaders; it does not speak for the DoD.

<sup>13</sup> Autonomous systems are designed to make complex decisions and function without continuous direction by a person.

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.

*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.*

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. At a minimum, a standard definition would help the DoD account for and subsequently govern its AI investments. The definition should consider the DoD's goals for using AI and should evolve as AI changes. Without a clear and standard AI definition, the DoD's AI oversight and governance could be applied inconsistently across the DoD.

### **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. It is essential for the JAIC to identify specific elements of information that require security

*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.*

protection to prevent adversaries from applying effective countermeasures to the AI capability. 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.<sup>14</sup> A properly constructed classification guide will enable accurate classification of AI information and help improve derivative classification decisions for AI information.<sup>15</sup> Table 2 shows the types of project information that require

<sup>14</sup> DoD Manual 5200.45, "Instructions for Developing Security Classification Guides," April 6, 2018.

<sup>15</sup> Derivative classification refers to the incorporating, paraphrasing, restating, or generating in new form information that is already classified, and marking the newly developed material consistent with the classification markings that apply to the source information.

security protections, if warranted, as defined by DoD Manual 5200.45. This type of information could also be used in AI projects. 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.

Table 2. Types of Information Used in AI Project That Should Be Protected\*

Performance and Capabilities	Specifications	Vulnerabilities	Procurement and Production	Operations
Altitude	Burn Rate	Countermeasures	Tactical Deployment	Location
Ballistics	Composition	Ground or Air Shock	Supply Plans and Status	Mission
Frequencies	Codes	Pressure	Progress/Schedule	Command and Control
Speed/Velocity	Energy Requirements	Infrared	Spare Parts	Environment
Reliability/Failure Rate	Payload	Electrical		
	Size, Weight, Shape			

Source: The DoD OIG.

\* This is not an all-inclusive list.

(FOUO) Personnel at several DoD Components that we assessed expressed concern with the proper protection of information used to support AI projects. For example, the lead electronics engineer for the Army AI project ██████████ stated that the biggest problem he faced related to governance of his project was the lack of a security classification guide. Specifically, the engineer stated that it was difficult to determine when publicly available information used to develop AI becomes DoD data and requires additional protection.

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.

### **Maintaining Accountability of and Collaborating on Artificial Intelligence 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.

*The RAND report acknowledges that the JAIC needs to maintain visibility of DoD AI activity, which includes accounting for DoD AI programs and projects.*

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.

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.

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.

### ***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. 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. 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. 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. 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.

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.

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.<sup>16</sup> 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.

### ***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. 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.

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

*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.*

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. 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. Although Federal and DoD standards may

<sup>16</sup> Office of Management and Budget, Memorandum M-19-19, "Update to Data Center Optimization Initiative," June 25, 2019.

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.

~~(FOUO)~~ A chief analyst for one of the six AI projects we assessed stated that the Marine Corps had processes for protecting the privacy of personal data used to support AI projects. The [REDACTED] will extract, process, analyze, transform, and enhance data sets used for AI models and algorithms.<sup>17</sup> A Navy AI program manager stated that DoD data should be stripped of sensitive or identifying information before being provided to contractors for the development of AI technology. In addition, the [REDACTED] [REDACTED] uses AI as an analytical tool to help senior leadership make decisions related to personnel retention, training, and mental health. A chief analyst for the Marine Corps stated that he implemented a process to remove personally identifiable information, such as names and birthdays, from large amounts of data before the data enter a contractor-led research environment.<sup>18</sup> While data are needed for AI technologies to function, when personal information is collected to support an AI technology, DoD Components and contractors must ensure that information is protected in accordance with existing privacy legislation. Without privacy standards related to the use of personally identifiable information, the DoD increases the risk of violating existing privacy laws if personal data are disclosed or accessed without consent from the individuals involved.

## Weaknesses in Management of AI Projects Could Threaten Our Military's Competitive Advantage

Developing a comprehensive governance framework during the emergence of AI will help fulfill the DoD's mission to protect the security of our Nation by developing and deploying advanced AI capabilities that ensure the United States sustains its competitive military advantage over its adversaries. An effective governance framework results in the ability to enforce compliance with decisions about technology use and procurement. In addition, an AI governance framework would allow the DoD to develop strong partnerships with commercial, academic, and international allies to help address global defense challenges.

<sup>17</sup> An algorithm is a process or set of rules to be followed in calculations or other problem-solving operation, especially by a computer.

<sup>18</sup> Personally identifiable information is any information that can be used to distinguish or trace a person's identity, such as date of birth, social security number, personal address, and biometric or medical records.



The lack of an AI governance framework decreases the DoD's ability to assess potential legal and privacy risks of injury and damage associated with using AI in an operational environment. Developing a central repository for data and tools increases the DoD's ability to decentralize, which would allow DoD Components to contribute to the quality of AI projects across the DoD and not just for a specific project. Without an AI inventory management process, the JAIC will face challenges accounting for, tracking, and monitoring AI projects. In addition, without a baseline, the JAIC will not be able to effectively govern the DoD's AI portfolio as required by the Deputy Secretary of Defense.

A standard definition of AI will also help the JAIC develop a baseline of AI projects. A security classification guide helps DoD Components communicate classification decisions, which is critical for ensuring users of data that support AI projects apply the appropriate level of protection. In addition, without a strategy for collaborating between DoD Components, the DoD's ability to analyze and collect data on patterns and trends in AI development will be limited. If the DoD does not develop an AI governance framework in a timely manner, there is an increased risk that the DoD will lose its opportunity to become a strong, technologically-advanced Department, which is essential for protecting U.S. service members; safeguarding U.S. citizens; defending allies and partners; and improving the affordability, effectiveness, and speed of our operations.

## **Management Comments on the Finding and Our Response**

### ***Army Artificial Intelligence Task Force Director Comments***

Although not required to comment, the Army AI Task Force Director, Army Futures Command, recommended that the JAIC develop and issue overarching guidance to the Services for protecting AI data and technology. He stated that a one-size-fits-all policy is not appropriate for collecting, managing, and sharing AI data or models, and that a spectrum of approaches is needed to protect AI data and technologies from fully releasable to highly classified. The Director also stated that different protection measures should apply for Army-sponsored university partners than deployed, operational systems, and that data stored and processed in commercial cloud environments need control measures in place, especially for remote access to data.

The Director added that the JAIC should consult with national-level governing bodies, such as the NIST, to develop protections for specific vulnerabilities of AI and machine learning systems that do not exist in regular information technology systems. He also stated that AI and machine learning systems are vulnerable to

adversarial attacks and that the behavior of AI systems cannot be predicted in every scenario, which creates gaps for exploitation of the systems. The Director stated that the protection of AI models is needed to prevent potential hackers from reverse engineering vulnerabilities of the model and aspects of the original data and that the protections should be maintained throughout the model's life cycle for mission critical systems.<sup>19</sup> Specific to the Army, the Director stated that the Army plans to develop an Enterprise Data Service Catalog to track Army data and their use in analytics. Lastly, the Director recommended that Army Regulation 530-1, "Operations Security," be updated to include the concept of counter AI, which is actions that friendly forces take to protect data that their formations generate and inadvertently release to opposing AI collection activities.<sup>20</sup>

### ***Our Response***

We agree that overarching guidance for protecting AI data and technology is needed. The development of a security classification guide specific to AI data will help DoD Components identify sensitive and classified information, and apply the appropriate security markings to ensure that information used to support AI projects is properly protected. As we state in this report, 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. Corrective action taken in response to Recommendation A.1.b should address the Director's concerns. The Director should forward his recommendation on updates to the Army Regulation 530-1 to the appropriate Army policy office.

## **Recommendations, Management Comments, and Our Response**

### ***General Comments on Recommendation A.1***

#### ***Department of Defense Chief Information Officer Comments***

The DoD CIO, responding for the JAIC Director, provided general comments on Recommendation A.1, stating that, while he was supportive of the DoD OIG's recommendations designed to strengthen the DoD's AI-related governance and data protection, the final report does not completely reflect a number of actions the JAIC took over the past year to enhance DoD-wide AI governance and to accelerate scaling AI and its impact across the DoD. The DoD CIO also stated that the JAIC provided the Deputy Secretary of Defense with an AI Implementation

<sup>19</sup> Reverse engineering is the duplication of another product by thorough examination to understand how the product works, and enhance or duplicate the product.

<sup>20</sup> Army Regulation 530-1, "Operation and Signal Security: Operations Security," September 26, 2014.

Plan that outlines the responsibilities, goals, objectives, and processes for fully implementing the DoD AI Strategy, which would allow responsible stewardship and synchronization of financial investments. He also stated that the plan includes chartering a DoD AI Executive Steering Group, a DoD AI Working Group, and nine AI subcommittees focused on the following areas—AI workforce; technical standards; enterprise infrastructure; test and evaluation; acquisition, academia, and industry engagement; responsible AI; international engagement; intelligence and security; and intelligent automation.

### ***Our Response***

We acknowledge in this report that the JAIC took steps to develop DoD-wide AI governance, such as adopting principles for the ethical use of AI within the DoD. However, we identified additional actions that are needed to develop and implement the AI governance framework. The intent of recommendation A.1 is to ensure that the elements identified in Finding A of this report are included in the DoD's AI governance framework.

### ***Recommendation A.1***

**We recommend that the Director of the Joint Artificial Intelligence Center establish an artificial intelligence governance framework that includes:**

- a. A standard definition of artificial intelligence that is updated at least annually.**

### ***Department of Defense Chief Information Officer Comments***

The DoD CIO, responding for the JAIC Director, partially agreed, stating that the JAIC acknowledges the importance of ensuring a common AI definition especially to improve accounting for AI investments, which helps DoD leaders make informed strategy and resource decisions. The DoD CIO stated that the DoD AI Executive Steering Group agreed with the JAIC's January 2019 recommendation to use the AI definition included in the 2018 DoD AI Strategy. The DoD CIO cited the 2019 RAND report, which challenged the benefit of a single AI definition, stating that the report concluded that enforcing a DoD-wide AI definition would likely be neither feasible nor helpful. The DoD CIO added that changing the AI definition would be counterproductive and does not align to any specific technical, operational, or programmatic requirement. Furthermore, the DoD CIO stated that the DoD AI Executive Steering Group is best postured to determine whether and when the DoD definition should be updated.

### ***Our Response***

Comments from the DoD CIO did not address the specifics of the recommendation; therefore, the recommendation is unresolved. Although the DoD CIO stated that the JAIC recommended using the AI definition included in the 2018 DoD AI Strategy, neither the DoD CIO nor the JAIC disseminated that decision to the DoD Components. As a result, the DoD Components we visited provided varying AI definitions that created a challenge in determining what is and is not considered an AI project, since many projects use some level of AI. While the DoD CIO seems to support the use of the AI definition from the 2018 AI Strategy, it also appears that he supports RAND's conclusion that a DoD-wide AI definition would not be helpful. As stated in this report, we disagree with RAND's conclusion and believe a standard AI definition is necessary to account for and subsequently govern the DoD's AI portfolio. Therefore, the JAIC should work with DoD Components to develop an AI definition that includes enough detail for Components to oversee, track, and manage their AI portfolios. The JAIC Director should provide additional comments on the final report to clarify the actions the JAIC will take to develop a standard AI definition.

### ***Deputy Chief of Naval Operations for Information Warfare Comments***

Although not required to comment, the Deputy Chief of Naval Operations for Information Warfare stated that a single AI definition risks being overly broad and recommended categorizing the definition into types or tiers based on the application. He also recommended that, if the DoD plans to use the definition for oversight or funding purposes, the definition should include sufficient details to assist the Military Services in identifying the correct definition.

### ***Our Response***

We agree that a single AI definition could be too broad and that the definition should include sufficient detail to allow DoD Components to oversee, track, and manage AI portfolios. As stated in our response to the DoD CIO, we are requesting additional comments on the final report to clarify the actions the JAIC will take to develop a standard AI definition. Corrective action taken in response to Recommendation A.1.a should address the Deputy Chief's concerns.

### ***Defense Threat Reduction Agency Integration Division Director for Research and Development Comments***

Although not required to comment, the DTRA Integration Division Director for Research and Development recommended that the JAIC develop a tiered definition of AI because a standard definition could require Components to implement all security standards regardless of the scale and type of AI project. The Director stated that a tiered definition would allow contractors to meet security standards for their level of AI research and not implement the full measure of security standards that are not applicable to the specific scale or type of investment.

### ***Our Response***

While we agree that a single definition of AI could be too broad, we disagree that a standard AI definition could require Components to implement all security standards regardless of the scale and type of AI project. NIST SP 800-53 states that organizations should tailor security controls to align with their mission, business requirements, and operational environments. Furthermore, NIST SP 800-171 requires risk assessments at the organization, mission, or system level; and at any phase in the system development life cycle, and that security controls be tailored to mitigate that risk. Tailoring security controls to the mission and system risks inherently results in the development of controls that will meet security standards based on the scale and type of AI project.

- b. A security classification guide to ensure consistent protection of data used and produced for AI projects.**

### ***Department of Defense Chief Information Officer Comments***

The DoD CIO, responding for the JAIC Director, partially agreed, stating that the DoD CIO and the JAIC agree that comprehensive AI security guidance is needed. The DoD CIO stated that the JAIC is developing a security classification guide, incorporating the lessons learned from the Project Maven guide, which was developed in 2017. He added that the Secretary of Defense delegated Original Classification Authority up to the top secret level to the JAIC Director and that the JAIC will use this authority during the development of the security classification guide for AI technologies.<sup>21</sup> However, the DoD CIO stated that when the JAIC uses data from other organizations, the JAIC will use that organization's classification

---

<sup>21</sup> Original Classification Authority is the authority to classify information owned or produced by a U.S. government agency. The original classification authority determines that the unauthorized disclosure of the information could reasonably be expected to result in damage to national security.

guidance unless the data is explicitly modified. The DoD CIO recommended deleting the words “used and” from Recommendation A.1.b and revising the recommendation to state, “A security classification guide to ensure consistent protection of data produced for AI projects.”

### ***Our Response***

Although the DoD CIO partially agreed, his plan to develop a security classification guide that will only apply to AI data that the JAIC produces or explicitly modifies does not meet the intent of the recommendation. Therefore, this recommendation is unresolved. The FY 2019 NDAA states that the designated official should develop classification guidance for **all AI-related activities** [emphasis added] for the DoD. As stated in this report, in October 2019, the Deputy Secretary of Defense formally designated the JAIC Director as the senior official to coordinate the DoD’s AI efforts. Therefore, the JAIC should develop a security classification guide specific to AI that will serve as the baseline for security classification guides developed by DoD Components maintaining AI projects. The JAIC Director should provide additional comments on the final report to clarify the actions the JAIC will take to develop a security classification guide.

### ***Deputy Chief of Naval Operations for Information Warfare Comments***

Although not required to comment, the Deputy Chief of Naval Operations for Information Warfare agreed and recommended that the JAIC develop a security classification guide that protects sensitive data and capabilities.

### ***Our Response***

We agree and the corrective action taken in response to Recommendation A.1.b should address the Deputy Chief’s recommendation.

- c. A baseline inventory of artificial intelligence projects ongoing within the DoD.**

### ***Department of Defense Chief Information Officer Comments***

The DoD CIO, responding for the JAIC Director, agreed, stating that in 2019, the JAIC coordinated with the CAPE on a DoD-wide data call to establish a baseline inventory of ongoing DoD AI projects. The DoD CIO stated that the baseline inventory was verified by the RAND report and further refined during the DoD OIG audit. The DoD CIO also stated that the JAIC will establish a biannual AI portfolio review with all DoD Components, with the first review scheduled for mid-2020.

### ***Our Response***

Comments from the DoD CIO addressed all specifics of the recommendation; therefore, the recommendation is resolved but will remain open. We will close the recommendation once the JAIC Director provides a copy of the refined baseline inventory that was completed during our audit and an explanation of the process used to verify the accuracy and completeness of the list.

- d. A process for identifying, monitoring, tracking, and reporting artificial intelligence projects, on a prescribed basis that also requires the DoD Military Services and Components to validate the resulting list of AI projects for accuracy.**

### ***Department of Defense Chief Information Officer Comments***

The DoD CIO, responding for the JAIC Director, agreed, stating that in August 2019, the DoD CIO published fiscal guidance that requires DoD Components to report AI investments in the annual Information Technology/Cyberspace Activities budget exhibit. The DoD CIO stated that the JAIC will establish a biannual AI portfolio review with all DoD Components, with the first review scheduled for mid-2020.

### ***Our Response***

Comments from the DoD CIO addressed all specifics of the recommendation; therefore, the recommendation is resolved but will remain open. We will close the recommendation once the JAIC Director provides the results of the JAIC's first AI portfolio review that shows AI projects were identified, monitored, tracked, and reported.

- e. A central repository for storing and sharing tools, data, policies, and procedures related to AI projects and technologies.**

### ***Department of Defense Chief Information Officer Comments***

The DoD CIO, responding for the JAIC Director, agreed, stating that the JAIC designed the Joint Common Foundation, which will provide a central repository for storing and sharing tools, data, policies, and procedures related to AI projects and technologies. The DoD CIO stated that the Joint Common Foundation will be a collaborative environment at multiple classification levels that will accelerate the development, testing, validation, and fielding of AI capabilities. He stated that the Joint Common Foundation will provide a repository for sharing source code, models, algorithms, and other artifacts, as well as access to leading-edge AI and machine learning tools, frameworks, and other shared resources, such as high performance computing centers, test networks and ranges, and Government and commercial cloud services.



### ***Our Response***

Comments from the DoD CIO addressed all specifics of the recommendation; therefore, the recommendation is resolved but will remain open. We will close the recommendation once the JAIC Director establishes the Joint Common Foundation repository, and the JAIC implements a process for updating the repository and disseminates that process to DoD Military Services and Components.

### ***Deputy Chief of Naval Operations for Information Warfare Comments***

Although not required to comment, the Deputy Chief of Naval Operations for Information Warfare recommended that the JAIC maintain and publish a set of related data categories included the central repository.

### ***Our Response***

We agree that data categories would be useful for the central repository. In his response to Recommendation A.1.d, the DoD CIO stated that the JAIC designed the Joint Common Foundation, which will provide a central repository for storing and sharing tools, data, policies, and procedures related to AI projects and technologies. Corrective action taken in response to Recommendation A.1.d should address the Deputy Chief's recommendation.

- f. Standards for assessing legal and privacy considerations when developing and using AI data and technologies.**

### ***Department of Defense Chief Information Officer Comments***

The DoD CIO, responding for the JAIC Director, partially agreed, stating that the DoD CIO and the JAIC agree with the importance of assessing legal and privacy considerations when developing and using AI data and technologies. However, the DoD CIO stated that there is no single standard that can be applied to legal and privacy considerations because every case is different, to varying degrees. The DoD CIO also stated that rather than developing standards, the JAIC recommends developing and following standard operating procedures and processes, in coordination with the appropriate legal counsel. In addition, the DoD CIO stated that the JAIC also wants to underscore the importance of responsible and ethical development and employment of AI technologies, as noted in the Secretary of Defense's February 21, 2020, memorandum, "Artificial Intelligence Principles for the Department of Defense." For those reasons, the DoD CIO stated that the JAIC recommends revising Recommendation A.1.f to read: "Standard operating procedures and processes, in coordination with the

appropriate Office of the Secretary of Defense offices, for assessing legal and privacy considerations when developing and using AI data and technologies; and guidance, recommendations, or policies for responsible and ethical development and use of AI data and technologies.”

### ***Our Response***

Although the DoD CIO partially agreed, his plan to work with legal counsel to develop standard operating procedures and processes for the responsible and ethical development of AI technologies meets the intent of the recommendation. Therefore, the recommendation is resolved but will remain open. We will close the recommendation once the JAIC Director provides a signed copy of the standard operating procedures.

We did not revise the recommendation as requested because the revision would not affect the substance of the recommendation. The development of standard operating procedures and processes will provide DoD Components and DoD contractors the necessary guidance for assessing the legal implications of using AI in an operational environment to prevent violations of current laws and civil liberties.

- g. A strategy for identifying similar artificial intelligence projects and promoting the collaboration of artificial intelligence efforts across the DoD.**

### ***Department of Defense Chief Information Officer Comments***

The DoD CIO, responding for the JAIC Director, agreed, stating that the planned personnel growth of the JAIC in FY 2021 would provide the resources required to improve visibility into DoD-wide AI projects; enhance collaboration on AI efforts; and support eliminating duplicative or nonperforming projects. The DoD CIO stated that the JAIC Missions Directorate would focus on early and frequent interaction with users and Service program offices. In addition, the DoD CIO stated that the DoD AI governance forums would improve insight into existing and proposed AI projects across the DoD. Furthermore, the DoD CIO stated that the JAIC will establish a biannual AI portfolio review with all DoD Components, with the first review scheduled for mid-2020.

### ***Our Response***

Comments from the DoD CIO addressed all specifics of the recommendation; therefore, the recommendation is resolved but will remain open. We will close the recommendation once the JAIC Director provides the strategy for identifying similar AI projects and collaborating across the DoD on those projects.

## Finding B

### Security Controls for Networks and Systems Supporting AI Projects Were Not Consistently Implemented

(FOUO) The four DoD Components and two contractors did not consistently implement security controls in accordance with Federal and DoD requirements for protecting data used to support AI projects and AI technologies from internal and external cyber threats. Specifically, for the four DoD Components we assessed, we found that:

- two DoD Components did not configure their systems to enforce the use of strong passwords;
- two DoD Components did not configure their networks and systems to generate system activity reports, nor did they review the networks and systems for malicious or unusual activity;
- one DoD Component did not configure user sessions to lock after periods of inactivity; and
- three DoD Components did not implement physical security controls, such as [REDACTED] AI data.

This occurred because the DoD Components we assessed did not establish processes to continually monitor the effectiveness of implemented security controls and assess the impact of missing security controls. The DoD requires its Components to protect DoD data by complying with applicable NIST Special Publication (SP) 800-53 (NIST SP 800-53) and DoD requirements; and periodically verify the implementation of security controls.<sup>22</sup> While the policies are not specific to AI, the requirements apply to all IT initiatives, including AI.

(FOUO) In addition, for the two DoD contractors we assessed, we found that:

- one contractor did not configure its systems to enforce the use of strong passwords;
- one contractor did not scan its network for viruses;
- one contractor did not consistently scan its network for vulnerabilities;
- one contractor did not configure its networks and systems to generate system activity reports;

<sup>22</sup> NIST SP 800-53, "Security and Privacy Controls for Information Systems and Organizations," Revision 4, January 22, 2015.

- two contractors configured user sessions to lock after extended periods and did not limit unsuccessful logon attempts to reduce the risk of malicious activities; and
- ~~(FOUO)~~ two contractors did not implement physical security controls, such as [REDACTED] AI data.

This occurred because DoD Component contracting agencies did not assess and verify whether DoD contractors complied with NIST SP 800-171 requirements for protecting DoD information before contract award and throughout the contract period of performance.<sup>23</sup> As a result, the DoD is at greater risk of becoming a victim of cyber attacks and compromising its AI data and technologies when DoD Components and contractors do not fully implement and verify compliance with applicable cyber security controls. Malicious actors can exploit vulnerabilities on the networks and systems of DoD Components and contractors and steal information related to some of the Nation's most valuable AI technologies. The disclosure of AI information developed by the DoD could threaten the safety of the warfighter and could cause the United States to be at a disadvantage against its adversaries.

## **DoD Components and Contractors Did Not Implement Security Controls to Protect AI Data and Technologies**

DoD Component and contractor controls and processes for networks and systems that support AI projects were insufficient to protect against potential unauthorized access to, or disclosure of, AI data and technologies. On March 14, 2014, the DoD CIO directed the DoD to implement NIST security controls to protect networks and systems. NIST SP 800-53 provides guidelines for security requirements for Federal information systems that process, store, or transmit data. NIST SP 800-171 lists security requirements for safeguarding sensitive information on non-Federal information systems. In a February 2019 memorandum, the Under Secretary of Defense for Acquisition and Sustainment stated that contracting offices could assess contractor system security plans to determine industry cybersecurity readiness for the contracts they administer. Therefore, the Military Services, DoD Components, and DoD contractors must implement security controls and processes to protect classified and unclassified AI information maintained on both DoD and non-DoD networks and systems in accordance with applicable criteria.

<sup>23</sup> NIST SP 800-171, "Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations," Revision 1, December 2016 (updated June 7, 2018).

To determine whether AI data and technologies were protected, we assessed cybersecurity controls, processes, and technology used for managing network and system authentication, vulnerabilities, and stored and transmitted data. In addition, we assessed physical security controls, such as gaining physical access to facilities that maintain DoD data. Based on our analyses and testing, we identified security weaknesses at all four DoD Components and the two contractor locations that we reviewed (see Table 3).

Table 3. Security Weaknesses Identified at DoD Components and Contractors

Security Weaknesses	Component/Contractor					
	Army	Marine Corps	SCO Contractor	Air Force	DTRA Contractor	Navy
Multifactor authentication and strong passwords not consistently used		X		X	X	
Subfolders not scanned for viruses			X			
Networks not scanned for vulnerabilities					X	
User activity not monitored	X	X	X			
System lockouts after inactivity were insufficient to prevent unauthorized access			X	X	X	
Physical security controls were not used to detect and prevent unauthorized access	X	X	X		X	X

Source: The DoD OIG.

### **Multifactor Authentication and Strong Passwords Not Consistently Used**

(FOUO) System administrators for the Marine Corps Directorate of Analytics and Performance Optimization (MCDAPO), Air Force Research Laboratory (AFRL), and the DTRA contractor did not configure systems that support AI projects to require multifactor authentication or [REDACTED].

DoD Instruction 8520.03 requires DoD Components to use multifactor authentication mechanisms, such as a Common Access Card (CAC) or a Rivest-Shamir-Adleman token (commonly known as RSA tokens), to access

(FOUO) DoD networks and systems.<sup>24</sup> In instances where multifactor authentication has not been implemented, the Defense Information Systems Agency (DISA) Security Technical Implementation Guide (STIG) for Application Security states that system passwords must be at least 15 characters in length and contain, at a minimum, a combination of uppercase letters, lowercase letters, numbers, and symbols. According to the MCDAPO chief analyst, there were no external or internal threats to the network because the systems were not connected to the Internet and he trusted the individuals working on the project. However, authorized personnel could easily pose an internal threat by committing malicious acts, such as fraud, theft, sabotage, espionage, or unauthorized disclosure.

(FOUO) The AFRL deputy chief scientist stated that the systems used to support the Air Force AI project reside on a non-DoD network. He stated that multifactor authentication was not used to access the network and there were [REDACTED]. He also stated that the project used open-source data that are readily available to the general public. The AFRL system administrator stated that, if the data become sensitive and require protection, the AFRL would move the project from the non-DoD network to the Defense Research and Engineering Network, which the audit team verified grants users access through multifactor authentication.<sup>25</sup> As the Air Force AI project continues to progress and collect data, there is an increased risk that the information maintained on the system could become sensitive, and how that information is accessed would not comply with DISA STIG requirements if AI project information remains on the non-DoD network.

(FOUO) The DTRA contractor system administrator did not fully enforce the use of multifactor authentication used to access the contractor's networks and systems supporting AI projects. Specifically, the system administrator did not enforce the use of multifactor authentication on workstations with [REDACTED]. The system administrator also stated that the DTRA contractor did not enforce password length and complexity requirements to access [REDACTED]. In addition, he stated that the contractor did not complete the [REDACTED] multifactor authentication on [REDACTED] but planned to complete the [REDACTED] by August 2020. NIST SP 800-171 requires DoD contractors maintaining DoD data to require users to access their network using multifactor authentication. The DoD requires system passwords to be at least 15 characters in length; however, this requirement does not apply to

<sup>24</sup> DoD Instruction 8520.03, "Identity Authentication for Information Systems," May 13, 2011, incorporating Change 1, July 27, 2017.

<sup>25</sup> Multifactor authentication uses two or more different factors to achieve authentication. Factors include something you know (for example, personal identification number or password), something you have (for example, cryptographic identification device or token), or something you are (for example, fingerprints or biometrics).

(FOUO) DoD contractors. The DoD CIO stated in response to recommendations from DoD OIG Report No. DODIG-2019-105, that specific password length and complexity requirements are left to the discretion of the contractor and that, if the DoD determines that the loss of confidentiality, integrity, or availability of DoD information could have a negative effect on organizational assets, more stringent passwords may be necessary.<sup>26</sup> Although NIST SP 800-171 does not specify a [REDACTED], DTRA should assess the ease with which a malicious actor could exploit passwords and should configure networks and systems to accept a [REDACTED] with the lowest probability of exploitation by a malicious actor.

Multifactor authentication and strong passwords are necessary because cyber attackers continuously attempt to gain access to networks, systems, and DoD data, and they use several methods to exploit weak passwords, such as dictionary attacks, phishing, and brute force attacks.<sup>27</sup> For example, a dictionary attack uses a simple file that contains words found in a dictionary. A cyber attacker randomly groups potential words based on the words in the dictionary file in an effort to guess user passwords. Some programs try to gain access to information systems by guessing common words and phrases, using personal information associated with specific users, or using a combination of various methods and programs to repeatedly attempt to access sensitive information.

**Subfolders Not Scanned for Viruses**

Although the SCO contractor used antivirus software to scan its network for viruses, it did not ensure that the virus scans included scans of subfolders within the files on the network. NIST SP 800-171 requires contractors to scan network folders for viruses. Industry best practices also include scanning all network subfolders for viruses. However, the system administrator for the SCO contractor did not configure the network to include all subfolders in the virus scans. Antivirus software should be configured to scan all hard drives and folders regularly to identify any file system infections. Not scanning files regularly introduces a higher risk of threats going undetected.

*However, the system administrator for the SCO contractor did not configure the network to include all subfolders in the virus scans.*

<sup>26</sup> DoD OIG Report No. DODIG-2019-105, "Audit of Protection of DoD Controlled Unclassified Information on Contractor-Owned Networks and Systems," July 23, 2019.

<sup>27</sup> Phishing is a method malicious actors use to pose as a reputable entity or person to obtain sensitive information, such as passwords and financial information. Brute force attacks are a trial and error method used to guess passwords.



Initially, the system administrator stated that he was unsure whether the antivirus scanning tool had the capability to scan subfolders. However, after the site visit, the audit team verified that the SCO contractor adjusted the antivirus scanning settings to include subfolders. Without thoroughly scanning networks for viruses, contractors increased the risk of malicious actions that could compromise critical AI programs. Although the SCO contractor that we assessed took corrective action, other SCO contractors may not be scanning subfolders for viruses.

### ***Networks Not Scanned for Vulnerabilities***

The DTRA contractor did not scan its networks to identify vulnerabilities. According to a network engineer for the DTRA contractor, he did not scan the contractor's network for vulnerabilities because the contractor had not developed a timeframe for installing scanning software on the workstations. NIST SP 800-171 requires contractors to periodically scan systems and applications to identify vulnerabilities, mitigate the vulnerabilities, and develop plans of action and milestones if they are unable to mitigate the vulnerabilities in a timely manner. Without knowing specific vulnerabilities affecting the contractor's network, the DTRA contractor could miss opportunities to address emerging threats and vulnerabilities, which increases the risk of the exposure or loss of sensitive data related to AI projects. Failure to patch systems will result in persisting vulnerabilities, which malicious actors could use to gain unauthorized access to a network and system, introduce malware, and exfiltrate controlled unclassified information. In a July 2018 speech at the Defense Systems Summit, the DoD CIO stated that the majority of cyber incidents are preventable with basic cyber hygiene. Regularly patching known vulnerabilities is part of basic cyber hygiene.

### ***User Activity Not Monitored***

(FOUO) System administrators for the Army [REDACTED], MCDAPO, and the SCO contractor did not [REDACTED]. The Army [REDACTED] system administrator stated that he did not have a [REDACTED]. He stated that user activity reviews could occur [REDACTED]. The MCDAPO system administrator stated that there was no full-time system administrator to [REDACTED]. In addition, the SCO contractor did not [REDACTED]. Although a director at the SCO contractor stated that he conducted quarterly reviews of user activity for new employees, he also stated that user activity reviews were [REDACTED].

DoD Directive 5205.16, "The DoD Insider Threat Program," states that DoD policy is to monitor user activity on DoD information networks and other sources as necessary and appropriate, to identify, mitigate, and counter insider threats.<sup>28</sup> Regularly monitoring user activity on networks could identify unauthorized access attempts and help prevent breaches. In addition, NIST SP 800-171 states that contractors should monitor for unlawful, unauthorized, or inappropriate system activity. When user activity is regularly monitored, organizations can identify unauthorized access attempts and activity, help prevent breaches, and provide forensic evidence when investigating malicious behavior. If system administrators do not consistently monitor user activity, DoD Components and DoD contractors will not be able to identify and correct improper or potentially illegal activity on their networks.

*If system administrators do not consistently monitor user activity, DoD Components and DoD contractors will not be able to identify and correct improper or potentially illegal activity on their networks.*

**System Lockouts After Inactivity Were Insufficient to Prevent Unauthorized Access**

(FOUO) System administrators for the AFRL and for the DTRA and SCO contractors did not [REDACTED]. The system administrator for the AFRL stated that he [REDACTED] because the AI project used open-source information that is readily available to the general public and therefore did not require protection. The DISA STIG for Application Security limits inactivity to 15 minutes before systems and networks automatically lock. In addition, NIST SP 800-171 requires user sessions to lock after a period of inactivity, though it does not specify the period. However, the system administrator for the DTRA contractor did not [REDACTED] because the [REDACTED]. The system administrator stated that the DTRA contractor plans to [REDACTED] by August 2020.

*The system administrator for the SCO contractor stated that when he set the lockout configuration, he did not confirm that the workstation would lock after 15 minutes of inactivity.*

(FOUO) Although the system administrator for the SCO contractor stated that he configured workstations to lock after 15 minutes of inactivity, we found that the workstations did not lock after more than [REDACTED] minutes of inactivity. The system administrator for the SCO contractor stated that when he set the lockout configuration,

<sup>28</sup> DoD Directive 5205.16, "The DoD Insider Threat Program," September 30, 2014 (incorporating Change 2, August 28, 2017).

(FOUO) he did not confirm that the workstation would lock after 15 minutes of inactivity. However, during the site visit, the SCO contractor reconfigured workstations to automatically lock after 15 minutes of inactivity, which aligns with DoD standards. Through observation, we verified that the workstations locked after 15 minutes of inactivity.

Without a network configuration that locks workstations after periods of inactivity, malicious cyber intruders could have unrestricted access to contractor systems that maintain data that support AI projects. Automatically locking systems and user accounts limits the potential for unauthorized access and prevents malicious actions that could jeopardize the confidentiality and integrity of sensitive data related to AI projects.

### ***Physical Security Controls Were Not Used to Detect and Prevent Unauthorized Access***

(FOUO) Security officials for the Army [REDACTED], MCDAPO, Naval Information Warfare Center (NIWC) [REDACTED] and the SCO contractor did not implement physical security measures to allow security personnel to [REDACTED] throughout facilities that maintained AI data and technologies. In addition, the DTRA contractor did not [REDACTED] AI data. Although the Army [REDACTED] to monitor physical access to the [REDACTED] facility where AI technology was developed, [REDACTED].

In addition, the image quality was grainy, which made it difficult to identify images clearly. According to the security specialist at the [REDACTED] facility, the [REDACTED] [REDACTED]. The NIWC [REDACTED] facility also did not [REDACTED].

[REDACTED] During our site visit to the NIWC [REDACTED] facility, the Integration Lead for the [REDACTED] project informed the audit team that the project was not using DoD data presently but that the project team planned on using DoD data in the future. Therefore, once the NIWC [REDACTED] starts using DoD data, it will be necessary for the NIWC [REDACTED] to monitor physical access to the facilities where DoD data are used. NIST SP 800-53 requires organizations to employ automated mechanisms, [REDACTED], to monitor, detect, and respond to suspicious physical access activities and incidents. Without [REDACTED], it would be difficult for physical security personnel at the NIWC [REDACTED] facility to promptly identify and respond to security incidents and suspicious activities [REDACTED].

(FOUO) The SCO contractor did not [REDACTED] AI project. In addition, the SCO contractor did not monitor the suite’s entrance and did not implement a process to identify visitors to the suite, such as visitor badges. NIST SP 800-171 requires organizations to protect and monitor the physical facility and support infrastructure for organizational systems. To meet the NIST requirement, NIST SP 800-53 suggests that active and timely [REDACTED], [REDACTED] is necessary to respond to suspicious activities and physical security incidents.<sup>29</sup> By not [REDACTED] with [REDACTED] to [REDACTED], the SCO contractor reduced its ability to promptly identify and respond to security incidents and suspicious activities [REDACTED].

The project manager at the MCDAPO facility did not secure the server room or the server racks used to store AI data. NIST SP 800-53 states that organizations should secure keys, combinations, and other physical access devices to areas that contain information system components, such as server rooms, media storage areas, and data and communication centers. Although access to the server room was controlled using a Common Access Card, we found that the master key to the server room was left unattended on a desk. The master key allowed the Common Access Card feature to be bypassed to gain access to the server room. According to the Marine Corps chief analyst, keys to the server room are supposed to be locked in a safe when not in use; however, he stated that he forgot to lock the keys up after he last used them. Failure to maintain proper control over access to the server room and server racks increases the risk that unauthorized individuals could access or tamper with servers that support network operations for AI programs. Locking server racks provides an additional layer of security to protect sensitive information from inappropriate activities of individuals inside the server room.

*Although access to the server room was controlled using a Common Access Card, we found that the master key to the server room was left unattended on a desk.*

(FOUO) In addition, the DTRA contractor did not [REDACTED] that maintain DoD AI information. NIST SP 800-171 requires organizations to protect and monitor the physical facility and support infrastructure for organizational systems. The DTRA contractor stated that the [REDACTED] were not locked because only authorized personnel could access the [REDACTED]. However, leaving [REDACTED] unlocked makes DoD AI information stored on the [REDACTED] vulnerable to insider threat.

<sup>29</sup> NIST SP 800-171 security controls are derived from the moderate security control baseline in NIST SP 800-53.

## The DoD's AI Data and Technologies Could Be Compromised by Cyber Attacks

Because DoD Components and contractors did not fully implement the security controls outlined in NIST SP 800-53 and NIST SP 800-171, DoD Components and contractors could become victims of cyber attacks.<sup>30</sup> Malicious actors could exploit vulnerabilities on the networks and systems and steal information related to some of the Nation's most valuable AI technologies. The protection of DoD AI data and technology is critical because AI will support military logistics, missile defense systems, and medical treatments for DoD personnel. The disclosure of AI information developed by the DoD could threaten the safety of the warfighter and could cause the United States to be at a disadvantage against our adversaries.

### Management Comments on the Finding and Our Response

#### *Deputy Chief of Naval Operations for Information Warfare Comments*

~~(FOUO)~~ The Deputy Chief of Naval Operations for Information Warfare disagreed that the NIWC [REDACTED] was noncompliant with the requirement to implement physical security controls to detect and prevent authorized access due to [REDACTED]. He stated that the security categorization level for NIWC [REDACTED] information technology assets (moderate for confidentiality; moderate for integrity; low for availability) only requires the NIWC [REDACTED].<sup>31</sup> The Deputy Chief stated that, for the NIWC [REDACTED], requiring [REDACTED] is a control enhancement; not a baseline, and that the NIST SP 800-53 allows organizations operating national security systems to use security controls and control enhancements voluntarily. He added that neither DoD nor Navy policy requires the implementation of physical security enhancements from NIST SP 800-53. Furthermore, the Deputy Chief requested that we update the report to show the Navy's compliance with NIST SP 800-53.

<sup>30</sup> A requiring activity is an organization that receives contracted support during operations.

<sup>31</sup> According to NIST SP 800-60, volume 1, revision 1, "Information Security: Guide for Mapping Types of Information and Information Systems to Security Categories," August 2008, the potential impact is moderate if the unauthorized disclosure, modification, or destruction of information is expected to have a serious adverse effect on organizational operations, assets, or individuals. The potential impact is low if the disruption of access to information is expected to have a limited adverse effect on organizational operations, assets, or individuals.

### *Our Response*

(FOUO) During our site visit to the NIWC [REDACTED], the Integration Lead for the [REDACTED] project informed the audit team that the project is a functional cloud environment that will store DoD data from other AI projects in the future. However, at the time of the site visit, the projects had yet to be incorporated in the [REDACTED] project. Therefore, once the NIWC [REDACTED] starts using DoD data from these AI projects, it will be necessary for the NIWC [REDACTED] to monitor physical access to the facilities where DoD data is used. DoD Instruction 8510.01 states that organizations must identify security baselines and if necessary, supplement the tailored baseline security controls with additional controls or control enhancements based on local conditions and risk assessments. NIST SP 800-53 requires organizations to employ automated mechanisms, [REDACTED], to monitor, detect, and respond to suspicious physical access activities and incidents. Without [REDACTED], it would be difficult for physical security personnel at the NIWC [REDACTED] facility to promptly identify and respond to security incidents and suspicious activities [REDACTED]. We made a minor revision on page 29 of this report to reflect the conversation held with the Integration Lead regarding the use of DoD data.

### *Defense Threat Reduction Agency Integration Division Director Comments*

The DTRA Integration Division Director for Research and Development, responding for the DTRA contracting officer, stated that he did not believe that contracting officers had the necessary skills to assess the impact to an organization of lost data. He stated that the program manager or the contracting officer's technical representative should possess the knowledge of IT systems, which would make them the most appropriate individuals to make such an assessment. The Director explained that project managers could track contractor compliance if a plan of action and milestones is required as a deliverable for any NIST SP 800-171 noncompliance items. He added that DTRA contracts containing information technology assets not under DTRA control are required to have a statement requiring NIST SP 800-171 compliance.

### *Our Response*

We agree that the contracting officer may not possess the necessary knowledge of cybersecurity to assess contractor compliance with NIST SP 800-171. Recommendation B.2 states that contracting officers, **in coordination with their DoD requiring activities**, [emphasis added] should develop and implement a plan to verify that contractors correct the weaknesses identified in this report. The Under Secretary of Defense for Acquisition and Sustainment

issued a memorandum in November 2018 that provides guidance for assessing contractor compliance with cybersecurity protections required by NIST SP 800-171.<sup>32</sup> Therefore, contracting officers and requiring activities should use the November 2018 memorandum to hold contractors accountable if they are not in compliance with NIST SP 800-171.

### ***Commanding General for the Army Combat Capabilities Development Command Comments***

(~~FOUO~~) Although not required to comment, the Commanding General of the Combat Capabilities Development Command (CCDC) stated that the [REDACTED] project may not be representative of the entire Army. The Commanding General stated that during the audit, the Command, Control, Communications, Computers, Cyber, Intelligence, Surveillance and Reconnaissance Center personnel informed the audit team that they were not processing classified or controlled unclassified data in the AI project identified. The Commanding General also stated that many of the security protocols are not required until the CCDC starts processing or storing classified AI data. He added that the audit team acknowledged this and informed the CCDC that the security protocols discussed during the site visit exit briefing were items for consideration and would not be considered findings until the facility processed classified data. The Commanding General stated that the findings cited in Table 3 [REDACTED] were resolved and demonstrated during the audit. He [REDACTED]

[REDACTED] The Commanding General also stated [REDACTED]

### ***Our Response***

(~~FOUO~~) While on site at the Command, Control, Communications, Computers, Cyber, Intelligence, Surveillance and Reconnaissance Center, the Army [REDACTED] Project Lead stated that the project was currently using open-source data that is readily available to the general public, but classified or controlled unclassified information could be used in the future. In addition, while on site we determined that a process existed to monitor user activity. However, as stated in this report, the Army [REDACTED] system administrator stated that user activity reviews could occur

<sup>32</sup> Under Secretary of Defense for Acquisition and Sustainment Memorandum, "Guidance for Assessing Compliance and Enhancing Protections Required by DFARS Clause 252.204.7012, Safeguarding Covered Defense Information and Cyber Incident Reporting," November 2018.



(FOUO) [REDACTED]  
[REDACTED].

We disagree that a [REDACTED] should be based on a [REDACTED]. Instead, a process for regularly monitoring all personnel is necessary to identify unauthorized access attempts and activity; prevent breaches; and provide forensic evidence when investigating malicious behavior. If system administrators do not consistently monitor user activity, DoD Components will not be able to identify and correct improper or potentially illegal activity on their networks.

## Recommendations, Management Comments, and Our Response

### ***Recommendation B.1***

We recommend that the Chief Information Officers for the Army, Marine Corps, Navy, and Air Force develop and implement a plan to correct the weaknesses identified at facilities that manage artificial intelligence projects related to:

- a. **Enforcing the use of multifactor authentication and strong passwords, when necessary, to reduce the risk of disclosing sensitive DoD information.**

### ***Army Cybersecurity and Information Assurance Director Comments***

The Cybersecurity and Information Assurance Director, responding for the Army CIO, agreed, stating that the Army implemented policy that requires the use of multifactor authentication or strong passwords at facilities that manage AI projects.

### ***Our Response***

Comments from the Cybersecurity and Information Assurance Director addressed all specifics of the recommendation; therefore, the recommendation is resolved but will remain open. We will close the recommendation once the Army CIO provides additional information on how he will ensure the enforcement of multifactor authentication or strong passwords at Army facilities that use AI data and technology.

### ***Marine Corps Deputy Commandant for Information Comments***

The Deputy Commandant for Information, responding for the Marine Corps CIO, agreed, stating that the Marine Corps enforces the use of multifactor authentication in accordance with DoD and Marine Corps policy, and that waivers for the use of multifactor authentication are reviewed by the Authorizing Official on a case-by case basis. She stated that if a system cannot support the use of multifactor authentication because of technical or operational constraints, the use of complex passwords is required.

~~(FOUO)~~ The Deputy Commandant stated that the systems administrator for the MCDAPO [REDACTED] system took action to ensure that access by laptops used on the closed network required strong passwords and that the system had a waiver for using multifactor authentication. She added that the effectiveness of cybersecurity programs, policies, and procedures are reviewed during monthly security evaluations, assessments, and Command Cyber Readiness Inspections and that appropriate corrective actions are taken if vulnerabilities or noncompliance is found. Furthermore, the Deputy Commandant stated that special attention would be put toward compliance with multifactor authentication and strong password requirements in upcoming cybersecurity assessments.

### ***Our Response***

Comments from the Deputy Commandant addressed all specifics of the recommendation; therefore, the recommendation is resolved but will remain open. We will close the recommendation once the Marine Corps CIO provides supporting documentation showing that she verified that the MCDAPO enforces the use of multifactor authentication and strong passwords, such the group policy setting for using multifactor authentication from the MCDAPO to the Marine Corps CIO.

### ***Air Force Associate Deputy Chief Information Officer Comments***

The Associate Deputy CIO, responding for the Air Force CIO, agreed, stating that the proper implementation of NIST SP 800-37 requirements could mitigate the security deficiencies listed in the recommendation.<sup>33</sup> The Associate Deputy CIO stated that he planned to publish a memorandum by July 1, 2020, to the Department of the Air Force Authorizing Officials emphasizing the need to properly follow applicable security guidance to protect AI systems.

<sup>33</sup> NIST SP 800-37, "Risk Management Framework for Information Systems and Organizations," Revision 2, December 2018. NIST SP 800-37 described the Risk Management Framework and managing security and privacy risks, and applying the framework to information systems and organizations.

### ***Our Response***

Comments from the Associate Deputy CIO addressed all specifics of the recommendation; therefore, the recommendation is resolved but will remain open. We will close the recommendation once the Air Force CIO provides the signed memorandum on the protection of AI systems and we verify that the memorandum includes guidance for enforcing the use of multifactor authentication and strong passwords.

- b. Regularly monitoring networks and systems to identify unusual user and system activity.**

### ***Army Cybersecurity and Information Assurance Director Comments***

The Cybersecurity and Information Assurance Director, responding for the Army CIO, agreed, stating that the Army has implemented policy, which requires Commanders to monitor unusual activity as part of a comprehensive cybersecurity program at facilities that manage AI projects.

### ***Our Response***

(FOUO) Comments from the Cybersecurity and Information Assurance Director addressed all specifics of the recommendation; therefore, the recommendation is resolved but will remain open. We will close the recommendation once we receive supporting documentation that the Army CIO verified that the system administrator for the Army ██████ monitor the network for unusual user and system activity on a consistent basis, such as monitoring notes from the Army ██████ to the Army CIO.

### ***Marine Corps Deputy Commandant for Information Comments***

The Deputy Commandant, responding for the Marine Corps CIO, agreed, stating that Marine Corps networks are continuously monitored with the use of intrusion detection and prevention systems. The Deputy Commandant stated that system and network administrators are responsible for monitoring user account and system activity; analyzing patterns of noncompliance or unauthorized activity; and taking appropriate administrative or programmatic actions to minimize security risks and insider threats.

(FOUO) The Deputy Commandant also stated that the system administrator for the MCDAPO ██████ took action to ensure daily monitoring of the servers occurs and that the times individuals access the system are recorded in logs that are maintained for users whose accounts are locked due to exceeding log in attempts. She added that users who have been “locked out” must be reset

(FOUO) by the administrator (no automatic re-enabling after a set time period expires is implemented). Lastly, she stated that the Marine Corps would give special attention toward ensuring all networks and systems are monitored to identify unusual user and system activity during upcoming cybersecurity assessments.

### ***Our Response***

Comments from the Deputy Commandant addressed all specifics of the recommendation; therefore, the recommendation is resolved but will remain open. We will close the recommendation once the Marine Corps CIO provides supporting documentation showing that she verified that the MCDAPO monitors the system for unusual user activity, such as monitoring notes from the MCDAPO to the Marine Corps CIO.

### ***Air Force Associate Deputy Chief Information Officer Comments***

The Associate Deputy CIO, responding for the Air Force CIO, agreed, stating that the proper implementation of NIST SP 800-37 requirements could mitigate the security deficiencies listed in the recommendation. The Associate Deputy CIO stated that he planned to publish a memorandum by July 1, 2020, to the Department of the Air Force Authorizing Officials emphasizing the need to properly follow applicable security guidance to protect AI systems.

### ***Our Response***

Comments from the Associate Deputy CIO addressed all specifics of the recommendation; therefore, the recommendation is resolved but will remain open. We will close the recommendation once the Air Force CIO provides a copy of the Associate Deputy CIO's memorandum on protecting AI systems issued to the Air Force Authorizing Officials and we verify that the memorandum includes guidance for regularly monitoring networks and systems to identify unusual user and system activity.

- c. Configuring all systems to lock automatically after 15 minutes of inactivity.**

### ***Army Cybersecurity and Information Assurance Director Comments***

The Cybersecurity and Information Assurance Director, responding for the Army CIO, agreed, stating that the Army implemented policy, which requires all facilities that manage AI projects to configure their systems to lock automatically after 15 minutes of inactivity, in accordance with DISA STIG requirements.

### ***Our Response***

Comments from the Cybersecurity and Information Assurance Director addressed all specifics of the recommendation; therefore, the recommendation is resolved but will remain open. We will close the recommendation once the Army CIO provides additional information describing how the Army will ensure that all facilities that use AI data and technology configure their systems to lock automatically after 15 minutes of inactivity.

### ***Marine Corps Deputy Commandant for Information Comments***

~~(FOUO)~~ The Deputy Commandant, responding for the Marine Corps CIO, agreed, stating that account lockout is enforced through a Group Policy Orchestrator update and that the Marine Corps requires information system security personnel to comply with DISA STIG requirements to lock out operating systems after periods of inactivity. She added that the MCDAPO [REDACTED] [REDACTED] complied with the recommendation at the time of the audit but that the Marine Corps would ensure special attention is put toward automatically locking all systems after 15 minutes of inactivity in upcoming cybersecurity assessments.

### ***Our Response***

Comments from the Deputy Commandant addressed all specifics of the recommendation. We confirmed during our site visit to MCDAPO that system accounts locked after 15 minutes of inactivity. We also agree with the Marine Corps CIO's action to ensure all systems automatically lock after inactivity in upcoming cybersecurity assessments. Therefore, the recommendation is closed and no further comments are required.

### ***Air Force Associate Deputy Chief Information Officer Comments***

The Associate Deputy CIO, responding for the Air Force CIO, agreed, stating that the proper implementation of NIST SP 800-37 requirements could mitigate the security deficiencies listed in in the recommendation. The Associate Deputy CIO stated that he planned to publish a memorandum by July 1, 2020, to the Department of the Air Force Authorizing Officials emphasizing the need to properly follow applicable security guidance to protect artificial intelligence systems.

### *Our Response*

Comments from the Associate Deputy CIO addressed all specifics of the recommendation; therefore, the recommendation is resolved but will remain open. We will close the recommendation once the Air Force CIO provides a copy of the Associate Deputy CIO's memorandum on protecting AI systems issued to the Air Force Authorizing Officials and we verify that the memorandum includes guidance for configuring systems to lock automatically after 15 minutes of inactivity.

- d. (FOUO) [REDACTED] to monitor personnel and respond to security incidents.

### *Army Cybersecurity and Information Assurance Director Comments*

The Cybersecurity and Information Assurance Director, responding for the Army CIO, agreed, stating that the Army implemented policy, which requires the Provost Marshal General to ensure the physical security program includes the measures required to safeguard information technology at facilities that manage AI projects.

### *Our Response*

(FOUO) Comments from the Cybersecurity and Information Assurance Director addressed all specifics of the recommendation; therefore, the recommendation is resolved but will remain open. We will close the recommendation once we receive supporting documentation from the Army CIO that the Provost Marshal General confirmed the [REDACTED] with [REDACTED], such as a completed [REDACTED] work order that includes [REDACTED].

### *Marine Corps Deputy Commandant for Information Comments*

(FOUO) The Deputy Commandant, responding for the Marine Corps CIO, agreed, stating that the Marine Corps Component Enterprise Data Centers have implemented appropriate physical security measures commensurate with applicable NIST SP 800-53 controls, to include [REDACTED]. She stated that the Marine Corps assessment and authorization process mandates compliance with the DoD's Risk Management Framework requirements to implement the appropriate NIST SP 800-53 security controls as prescribed by the Committee on National Security Systems Instruction 1253, "Security Categorization and Control Selection for National Information Systems." The Deputy Commandant also stated that the MCDAPO [REDACTED] complied with the recommendation

(FOUO) at the time of the audit. In addition, the Deputy Commandant stated that the Marine Corps would put special attention toward ensuring facilities hosting information technology systems have the appropriate physical security controls implemented based on their security categorization as required by DoD policy.

### ***Our Response***

(FOUO) Comments from the Deputy Commandant addressed all specifics of the recommendation. We confirmed during our site visit to MCDAPO, that the Marine Corps [REDACTED]. We also agree with the Deputy Commandant's plans to ensure facilities hosting information technology systems have the appropriate physical security controls implemented. Therefore, the recommendation is closed and no further comments are required.

### ***Air Force Associate Deputy Chief Information Officer Comments***

The Associate Deputy CIO, responding for the Air Force CIO, agreed, stating that the proper implementation of NIST SP 800-37 requirements could mitigate the security deficiencies listed in the recommendation. The Associate Deputy CIO stated that he would publish a memorandum by July 1, 2020, to the Department of the Air Force Authorizing Officials emphasizing the need to properly follow applicable security guidance to protect AI systems.

### ***Our Response***

(FOUO) Comments from the Associate Deputy CIO addressed all specifics of the recommendation; therefore, the recommendation is resolved but will remain open. We will close the recommendation once the Air Force CIO provides a copy of the memorandum and we verify that the memorandum includes guidance [REDACTED] [REDACTED] to monitor personnel and respond to security incidents.

### ***Army Commanding General for the Combat Capabilities Development Command Comments***

(FOUO) Although not required to comment, the Army Commanding General for the CCDC agreed, stating that during the site visit to CCDC, the audit team noted that the [REDACTED] in the Command, Control, Communications, Computers, Cyber, Intelligence, Surveillance and Reconnaissance Center could not [REDACTED] [REDACTED] where the AI data were stored and AI research was performed. The Commanding General also stated that on October 2019, the CCDC informed DoD OIG that [REDACTED] was operational. In addition, the Commanding General stated that the research building in question is access-controlled and within a secure facility that requires badge access for entry.



### ***Our Response***

~~(FOUO)~~ We acknowledge the CCDC Commanding General's statement that the CCDC informed the audit team in October 2019 that [REDACTED] was operational; however, we have not been able to verify the ability of [REDACTED]. As stated in our response to the Army CIO, we are requesting supporting documentation that the Provost Marshal General confirmed the [REDACTED] [REDACTED] with [REDACTED], such as a completed [REDACTED] work order that includes [REDACTED]. Corrective action taken by the Army CIO in response to Recommendation B.1.d should address the Commanding General's concerns.

- e. **Securing data centers, server racks, and associated keys.**

### ***Army Cybersecurity and Information Assurance Director Comments***

The Cybersecurity and Information Assurance Director, responding for the Army CIO, agreed, stating that the Army implemented policy, which requires that facilities that manage AI projects implement security controls contained in the NIST SP 800-53.

### ***Our Response***

Comments from the Cybersecurity and Information Assurance Director addressed all specifics of the recommendation; therefore, the recommendation is resolved but will remain open. We will close the recommendation once the Army CIO provides the policy implemented by the Army that requires facilities that use AI data and technology to secure the data centers, server racks, and associated keys.

### ***Marine Corps Deputy Commandant for Information Comments***

~~(FOUO)~~ The Deputy Commandant, responding for the Marine Corps CIO, agreed, stating that Marine Corps Component Enterprise Data Centers are secured by badge-only access in accordance with applicable Federal, NIST, Department of Navy, and Marine Corps policies. She stated that physical keys are secured in Federal-approved safes/lockboxes and that the server room for the MCDAPO [REDACTED] is within a Sensitive Compartmented Information Facility and requires CAC-enabled access using keypad and number combination. The Deputy Commandant stated that the master key to the room is locked in a safe when not in use. She also stated that the Marine Corps would put special attention toward ensuring facilities hosting information technology systems have the appropriate physical security controls implemented based on their security categorization as required by DoD policy.

### ***Our Response***

Comments from the Deputy Commandant addressed all specifics of the recommendation; therefore, the recommendation is resolved but will remain open. We will close the recommendation once the Marine Corps CIO provides supporting documentation showing that the MCDAPO secures data centers, server racks, and associated keys, such as written confirmation from the MCDAPO to the Marine Corps CIO.

### ***Air Force Associate Deputy Chief Information Officer Comments***

The Associate Deputy CIO, responding for the Air Force CIO, agreed, stating that the proper implementation of the NIST SP 800-37 requirements could mitigate the security deficiencies listed in the recommendation. The Associate Deputy CIO stated that he would draft a memorandum by July 1, 2020, to Department of the Air Force Authorizing Officials emphasizing the need to properly follow applicable security guidance to protect artificial intelligence systems.

### ***Our Response***

Comments from the Associate Deputy CIO addressed all specifics of the recommendation; therefore, the recommendation is resolved but will remain open. We will close the recommendation once the Air Force CIO provides a copy of the Associate Deputy CIO's memorandum on protecting AI systems issued to the Air Force Authorizing Officials.

## **Management Comments Required**

Although Deputy Chief of Naval Operations, responding for the NAVY CIO, stated that the Navy disagreed with the finding related to physical security, he did not respond specifically to Recommendations B.1.a, B.1.b, B.1.c, B.1.d, and B.1.e. Therefore, the recommendations are unresolved. We request that the Navy CIO provide comments on the final report that describe the action he will take (or has taken) to resolve the recommendations.

## **Recommendation B.2**

### ***Strategic Capabilities Office Director Comments***

The SCO Director provided general comments on Recommendation B.2, stating that the SCO does not directly award or administer contracting actions for its programs and that the SCO exercises acquisition authorities through a Military Department, a DoD contract administration services component, or a Federal department and agency. He stated that although SCO is reviewing options for obtaining contracting authority, the contract for the audited contractor was awarded by the Department

of the Interior, Interior Business Center. The SCO Director also stated that the contractor was awarded an “other transaction-prototype agreement,” which is not a Federal Acquisition Regulations-based contract. However, he stated that, under the agreement, the SCO Security and Program Protection Directorate is responsible for providing oversight and guidance over security authorities over all aspects of program protection, including information security, cybersecurity, and physical security.

### ***Our Response***

We agree with the SCO Director that although SCO does not have contracting authority, as the requiring activity, the SCO Security and Program Protection Directorate is responsible for information security, cybersecurity, and physical security.

### ***Redirected Recommendation***

As a result of management comments, we redirected Recommendation B.2 from the contracting officer for the Strategic Capabilities Office to the Strategic Capabilities Office Security and Program Protection Director, who has the authority to implement the recommendation.

### ***Recommendation B.2***

**We recommend that contracting officer for the Defense Threat Reduction Agency and the Strategic Capabilities Office Security and Program Protection Director, in coordination with their DoD requiring activities, develop and implement a plan to verify that contractors correct the weaknesses identified in this report related to:**

- a. **Assessing whether the loss of confidentiality, integrity, or availability of DoD information could have a negative effect on organizational assets, and requiring contractors to use multifactor authentication or configuring its systems to meet the minimum DoD password length and complexity requirements.**

### ***Defense Threat Reduction Agency Integration Division Director Comments***

The Integration Division Director for DTRA’s Research and Development Directorate, responding for the DTRA Contracting Officer, agreed, stating that the contracting officer’s representative verified that the contractor started implementing multifactor authentication controls by requiring the use of RSA tokens, which will no longer require users to enter passwords to access contractor systems.

### ***Our Response***

Comments from the Division Director addressed all specifics of the recommendation; therefore, the recommendation is resolved but will remain open. We will close the recommendation once the DTRA Contracting Officer provides documentation verifying that the contractor fully implemented the use of RSA tokens, such as the group policy setting from the contractor that shows RSA tokens are required to access the contractor systems.

#### **b. Scanning networks, including subfolders, for viruses.**

### ***Strategic Capabilities Office Director Comments***

The SCO Director, responding for the Security and Program Protection Director, agreed, stating that although SCO does not have contracting authorities, SCO's Program Security Representatives would continue monitoring and verifying contractor compliance through quarterly program reviews and spot checks to ensure contractors consistently scan networks, to include all subfolders, with anti-virus software. The SCO Director also stated that the contractor corrected the issue by configuring the anti-virus software to scan all network subfolders. In addition, the SCO Director stated that the contractor logged corrective actions and incorporated the actions in standard operating procedures, which were provided to the audit team. Furthermore, the SCO Director stated that the contractor scanned the network and identified no abnormalities within all folders and subfolders. Lastly, the SCO Director stated that, since the audit, SCO's program security representative and the program manager participate in the quarterly program reviews and conduct spot checks to ensure anti-virus scans are conducted in accordance with standard operating procedures.

### ***Our Response***

Comments from the SCO Director addressed all specifics of the recommendation. We confirmed after our site visit that SCO configured the anti-virus software to scan all network subfolders. We agree with the program security representative and the program manager's participation in the quarterly program reviews and spot checks to ensure anti-virus scans are conducted. Therefore, the recommendation is closed and no further comments are required.

**c. Identifying and mitigating vulnerabilities in a timely manner.**

***Defense Threat Reduction Agency Integration Division  
Director Comments***

(~~FOUO~~) The Integration Division Director for DTRA's Research and Development Directorate, responding for the DTRA Contracting Officer, agreed, stating that the contracting officer's representative verified that the contractor scans its network weekly, although the [REDACTED] were initially not included in those scans. The Director stated that the contractor has since set up accounts on the [REDACTED] to include them as part of the weekly scans. In addition, the Director stated that the contractor reviews the results of network scans manually and that the contractor was on track for implementing NIST SP 800-171 information technology security compliance this year.

***Our Response***

(~~FOUO~~) Comments from the Division Director addressed all specifics of the recommendation; therefore, the recommendation is resolved but will remain open. We will close the recommendation once the DTRA Contracting Officer provides documentation verifying that the contractor scans the [REDACTED] for vulnerabilities and mitigates the vulnerabilities in a timely manner, such as scan results and plan of actions and milestones.

**d. Regularly monitoring networks and systems to identify unusual user and system activity.**

***Strategic Capabilities Office Director Comments***

The SCO Director, responding for the Security and Program Protection Director agreed, stating that although SCO does not have contracting authorities, SCO's Security and Program Protection Directorate would continue to ensure that contractors supporting SCO AI projects incorporate network monitoring into program specific protection plans. The SCO Director stated that corrective actions were taken on the spot and the contractor was monitoring all persons associated with the program and their actions while on the local network. The SCO Director also stated that standard operating procedures were updated to ensure the network where information is hosted is regularly scanned for vulnerabilities and anomalies in user behavior. In addition, the SCO Director stated that, since the audit, the program security representative conducts quarterly program reviews and that post-audit monitoring has not identified any abnormalities in the network and systems.

### ***Our Response***

Comments from the SCO Director addressed all specifics of the recommendation; therefore, the recommendation is resolved but will remain open. We will close the recommendation once the Security and Program Protection Director provides a copy of the updated standard operating procedures, and supporting documentation verifying that the contractor monitors and reviews system activity on a regular basis, such as scan results and plan of actions and milestones.

- e. **Using an automatic system lockout after inactivity.**

### ***Defense Threat Reduction Agency Integration Division Director Comments***

The Integration Division Director for DTRA's Research and Development Directorate, responding for the DTRA Contracting Officer, agreed, stating that the contracting officer's representative verified that the contractor resolved the automatic system lockout issue.

### ***Our Response***

Comments from the Division Director addressed all specifics of the recommendation; therefore, the recommendation is resolved but will remain open. We will close the recommendation once the DTRA Contracting Officer provides documentation verifying that the contractor is automatically locking systems after inactivity, such as the group policy setting for system lockouts.

- f. **(FOUO) [REDACTED] to monitor personnel and respond to security incidents.**

### ***Strategic Capabilities Office Director Comments***

(FOUO) The SCO Director, responding for the Security and Program Protection Director, disagreed, stating that [REDACTED] is not a requirement of NIST SP 800-53. He stated that a security site survey determined that the [REDACTED] in place for the building sufficiently satisfied program security requirements, which includes [REDACTED] and roving security that includes local law enforcement. In addition, he stated that security personnel monitor the work site 24 hours a day, 7 days a week, and that they respond to any alarms or indications of forced entry. He stated that external and internal doors have badge readers that log access by individual, and that the [REDACTED] are located behind double-locked doors that require a badge and physical key to access. Furthermore, the SCO Director stated that a program security representative assessed the security posture at the entry point to the [REDACTED]

(FOUO) [REDACTED] and determined that it was not fiscally prudent to require the contractor to [REDACTED]. Lastly, the SCO Director stated that the program manager and program security representative ensured that visitor badges and logs are on site and are being used to track all visitors.

### *Our Response*

(FOUO) Comments from the SCO Director did not address the specifics of the recommendation; therefore, the recommendation is unresolved. While we acknowledge that the SCO contractor has multiple layers of protection, such as badged access to facilities we visited and a 24/7 roving patrol outside of the facility, it did not have controls in place for the support infrastructure where DoD data resided. The NIST SP 800-171 requires organizations to protect and monitor both the physical facility and support infrastructure. Although the [REDACTED] resided [REDACTED], there was no mechanism for monitoring access to the [REDACTED]. Since [REDACTED] are part of the contractor's support infrastructure, [REDACTED] [REDACTED] to monitor access to the [REDACTED]. Failing to [REDACTED] leaves a gap in the ability [REDACTED] who access the [REDACTED] within the SCO contractor facility. This includes monitoring insider threats posed by individuals who are authorized to access the controlled areas. A roving patrol can quickly respond to an intrusion in real time when alerted in a timely manner, the officer could miss an incident in an area that he or she recently patrolled. The use of [REDACTED] [REDACTED]. In addition, [REDACTED] would help to identify whether individuals accessed the facility without using their access cards, which would not show up on the records of the access control card reader. The Security and Program Protection Director should provide additional comments describing how and when he will implement the recommendation, or provide signed documentation from the SCO CIO accepting the risk of not [REDACTED].



- g. Implementing physical security safeguards for server rooms, server racks, and associated keys.**

***Defense Threat Reduction Agency Integration Division  
Director Comments***

The Integration Division Director for DTRA's Research and Development Directorate, responding for the DTRA Contracting Officer, agreed, stating that the contracting officer's representative verified that the contractor added physical locks to the server racks in the server room.

***Our Response***

Comments from the Integration Division Director addressed all specifics of the recommendation; therefore, the recommendation is resolved but will remain open. We will close the recommendation once the DTRA Contracting Officer provides documentation verifying that the contractor installed physical locks to server racks, such as site visit notes of a visual verification of the installed locks.

## Appendix A

---

### Scope and Methodology

We conducted this performance audit from April 2019 through March 2020 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.

To determine the DoD's progress in developing an AI governance framework and standards, we interviewed officials from the Army, Navy, Air Force, Office of the Under Secretary of Defense for Research and Engineering, Office of the DoD CIO, Defense Advanced Research Projects Agency, JAIC, SCO, and Defense Innovation Unit. To determine the effectiveness of security controls in place to protect AI data and technologies, we interviewed project managers, system administrators, and security officers to identify security protocols implemented to protect DoD AI data. Additionally, we reviewed Federal laws and DoD policy concerning AI, information security, and data protection.

We received a list of DoD AI projects from CAPE. To verify the accuracy of the list, we sent a data call to the DoD Components to review and verify the project names, project descriptions, funding amounts, and points of contact. We compiled a list of AI projects from the data call responses and selected a nonstatistical sample of 6 of 446 AI projects managed by both DoD Components and DoD contractors. See Appendix C for the sampling approach for selecting the six site visit locations. Of the six AI projects selected, we evaluated the effectiveness of security controls that were implemented to protect AI data and technologies. Table 4 lists the six AI projects and the associated DoD Component.

Table 4. (FOUO) Artificial Intelligence Projects and Associated DoD Components

(FOUO) Artificial Intelligence Project	Associated DoD Component
[REDACTED]	Army Intelligence and Information Warfare Directorate
[REDACTED]	Marine Corps Directorate of Analytics and Performance Optimization
[REDACTED]	Navy Information Warfare Center [REDACTED]
[REDACTED]	Air Force Research Laboratory
[REDACTED]	SCO Contractor
[REDACTED]	DTRA Contractor

(FOUO)

Source: The DoD OIG.

## Use of Computer-Processed Data

We reviewed a list of AI projects compiled by CAPE to determine the total number of AI project across the DoD. CAPE personnel provided us the list of AI projects in a Microsoft Excel worksheet. According to CAPE, a data call was performed to identify AI projects across the DoD. We determined that the list of AI projects compiled by CAPE was not sufficiently reliable to determine the total number of AI projects within the DoD. CAPE’s list identified 456 projects ranging from unclassified to Secret. However, we identified instances where AI projects included in the project list developed by CAPE were no longer active. Therefore, we conducted a data call to DoD Components to identify AI projects as of April 2019. Our data call identified 446 AI projects. We used the results of our data call to select a sample of AI projects to assess. See Appendix C for details on the sampling methodology.

(FOUO) We used computer-processed data extracted from the MCDAPO [REDACTED] [REDACTED] to generate a list of users of the network used for the AI project at the Marine Corps facility visited. To assess the reliability of the list, we compared user data to the list of authorized users and the project’s roster to determine whether those who accessed the MCDAPO [REDACTED] were authorized users and that their user privileges aligned with their job responsibilities. We confirmed that all users who accessed the MCDAPO [REDACTED] were authorized users and that their user privileges were consistent with their job responsibilities. Therefore, the system-generated list of users was sufficiently reliable to test whether a user’s justification for access to networks used for the AI project was appropriate.

## Use of Technical Assistance

The DoD Quantitative Methods Division provided assistance in developing the nonstatistical sampling methodology to select the six site visit locations for Finding B. See Appendix C for more details on the sampling methodology.

## Prior Coverage

During the last 5 years, the Government Accountability Office (GAO) issued two reports and the DoD OIG issued two reports discussing AI. Unrestricted DoD OIG reports can be accessed at <http://www.dodig.mil/reports.html/>.

### **GAO**

GAO-19-161, “Federal Agencies Should Take Additional Steps to Prepare for Potential Workforce Effects,” March 7, 2019

This report discusses automated vehicle technology and focuses on when the technology would affect the commercial trucking industry and how adopting such technology would affect the future workforce. The GAO reviewed research papers on automated trucking technology, viewed demonstrations of the technology, and analyzed Federal data on the truck driver workforce. The GAO also interviewed officials from the Departments of Transportation and Labor, as well as a range of stakeholders, including technology developers, companies operating their own trucking fleets, truck driver training schools, truck driver associations, and workforce development boards. The GAO found that automated driving technology has the potential to drastically reduce, and possibly even eventually eliminate, the need for human drivers in the commercial trucking industry in the not too distant future.

GAO-18-142SP, “Artificial Intelligence: Emerging Opportunities, Challenges, and Implications,” March 28, 2018

The GAO report identifies opportunities and challenges related to AI based on discussions held at a forum convened by the Comptroller General. The forum focused on the prospects for using AI in the near future and identified areas where the Government needs to revise policy and research priorities, such as safety and security; ethics; and training and education. The report concluded that the four biggest challenges in AI include data collection, the need for specific high-skilled labor, protecting civil liberties, and developing an ethical framework to govern the use of AI. The GAO reported that AI investments could significantly support the DoD in identifying and patching vulnerabilities, as well as detecting and defending against cyber attacks.

**DoD OIG**

DODIG-2019-105, "Audit of Protection of DoD Controlled Unclassified Information on Contractor-Owned Networks and Systems," July 23, 2019

The DoD OIG determined that DoD contractors did not consistently implement DoD-mandated system security controls for safeguarding Defense information. In addition, DoD Component contracting offices and requiring activities did not verify that contractors' networks and systems met security requirements or that contractors implemented minimum security controls for protecting controlled unclassified information. Furthermore, DoD Component contracting offices and requiring activities did not implement processes and procedures to track which contractors maintain controlled unclassified information on their networks and systems.

"Fiscal Year 2019 Top DoD Management Challenges," November 15, 2018

The DoD OIG's FY 2019 Top Management Challenges report contains multiple references to AI and its future use by the DoD and its adversaries. The report states that China, in particular, is investing heavily in AI to surpass the United States in AI dominance, although the DoD is taking steps to counter the threat. For example, the report states that the Office of the DoD CIO established the JAIC as the centralized office within the DoD to accelerate the delivery of AI and synchronize DoD efforts.

## Appendix B

### Timeline of JAIC Key Activities

Table 5 shows a timeline of JAIC key activities from the establishment of the JAIC through the expected full operational capability date.

Table 5. ~~(FOUO)~~ Timeline of JAIC Key Activities

<del>(FOUO)</del> Date	Event
January 3, 2018	Congress meets to establish FY 2019 NDAA. Section 238 of the FY 2019 NDAA relates to the Joint AI Research, Development, and Transition activities within the DoD.
June 27, 2018	The DoD issues the 2018 DoD Artificial Intelligence Strategy. The Strategy articulates the DoD’s approach and methodology for incorporating AI-enabled capabilities within the DoD.
June 27, 2018	The Deputy Secretary of Defense issues a memorandum establishing the JAIC. The memorandum directs the DoD CIO to provide a list of initial NMIs, proposed resourcing plans for both FY 2018 and 2019, and personnel needs by July 27, 2018. The list of initial NMIs was supposed to be launched by September 25, 2018.
July 27, 2018	The list of initial NMIs, proposed resourcing plans for FY 2018 and FY 2019, and personnel needs are due. We requested, but the JAIC did not provide, the JAIC’s reporting information for FY 2018. Therefore, we could not determine whether it was submitted. The remaining items were not submitted until September 28, 2018.
August 13, 2018	The FY 2019 NDAA is signed by the President and becomes law. Within 1 year, the Secretary of Defense shall designate a senior official of the DoD to coordinate activities relating to the development of AI, and define AI for use within the DoD.
September 11, 2018	The Deputy Secretary of Defense issues a memorandum directing the DoD CIO to establish a JAIC Implementation Team. The memorandum requests additional personnel resources to support the JAIC Implementation Team. The goal is to launch a provisional JAIC by January 1, 2019, and for the JAIC to become fully operational by October 1, 2019. For the purpose of this report, the provisional JAIC is staffed with detailed personnel from across the DoD, and a fully functional JAIC is staffed with permanent personnel. However, neither deadline was met.
September 28, 2018	The list of initial NMIs related to humanitarian assistance, disaster relief, and predictive maintenance is published.
December 7, 2018	The JAIC commissions RAND to conduct an independent study to assess the DoD’s AI posture.
December 12, 2018	The Senate confirms Lieutenant General Shanahan as the JAIC Director.
February 12, 2019	The DoD issues its “Summary of the 2018 DoD AI Strategy,” which directs the DoD to accelerate the use of AI. The JAIC is identified as the focal point to carry out the DoD AI Strategy.

~~(FOUO)~~

~~(FOUO)~~ *Timeline of JAIC Key Activities (cont'd)*

<del>(FOUO)</del> Date	Event
August 13, 2019	The FY 2019 NDAA requires the Secretary of Defense to designate a senior official to coordinate activities relating to AI by this date; and define AI for use within the DoD.
October 2, 2019	The Deputy Secretary of Defense designates the JAIC Director as the senior official responsible for coordinating AI activities within the DoD. The Deputy Secretary of Defense requires the JAIC Director to provide a plan that includes a formal DoD AI policy, a delineation of roles and responsibilities, and a formal AI governance structure no later than March 30, 2020. The JAIC Director must coordinate with the Technical Director of the Office of the Under Secretary of Defense for Research and Engineering on this tasker.
November 7, 2019	The JAIC provides the DoD OIG with a draft memorandum to establish an AI Executive Steering Group to provide guidance and oversight of AI policy. The AI Executive Steering Group will be a senior oversight body that will bring leaders together to advance policies and initiatives to accelerate the integration of AI technologies.
December 17, 2019	RAND issues report "The Department of Defense Posture for Artificial Intelligence: Assessment and Recommendations," which assesses the state of AI within the DoD.
March 30, 2020 (Projected)	The JAIC is required to deliver the AI Implementation Plan to the Deputy Secretary of Defense based on the October 2, 2019, memorandum.
June 30, 2020 (Projected)	The DoD CIO expects the JAIC to be fully staffed. The DoD CIO also expects the JAIC to fully implement an AI governance framework.
[REDACTED] (Projected)	The [REDACTED] plans to issue an [REDACTED]. <span style="float: right;"><del>(FOUO)</del></span>

Source: The DoD OIG.



## Appendix C

---

### Sampling Approach

We used a nonstatistical sampling technique to select the six site visit locations. In March 2019, the audit team received a list from CAPE of 456 AI projects throughout the DoD. Because the CAPE list was almost a year old, we worked with the DoD Components to verify the accuracy of the list before we selected our sample. The following 18 DoD Components had AI projects listed in the updated list.

- U.S. Army
- U.S. Marine Corps
- U.S. Navy
- U.S. Air Force
- Office of the Under Secretary of Defense for Research and Engineering
- Office of the Under Secretary of Defense for Personnel and Readiness
- Office of the Under Secretary of Defense for Intelligence
- U.S. Special Operations Command
- U.S. Transportation Command
- Cost Assessment and Program Evaluation
- Chief Management Officer of the Department of Defense
- Defense Advanced Research Projects Agency
- Defense Intelligence Agency
- Defense Threat Reduction Agency
- Missile Defense Agency
- Combating Terrorism Technical Support Office
- Office of Net Assessment
- Strategic Capabilities Office

The audit team consolidated the responses from the DoD Components and placed the projects into six categories:

- U.S. Army;
- U.S. Marine Corps;
- U.S. Navy;

- U.S. Air Force;
- Defense Agencies and Field Activities; and
- Research and Academia.

We selected a nonstatistical sample from the universe of projects using the “RAND” function in Microsoft Excel to eliminate selection bias. Next, the audit team selected the first project in the randomized list for that category. The audit team repeated this methodology for each category in the list, resulting in a sample of six projects. We contacted the project managers for the selected projects and determined that some projects did not meet the NDAA definition of an AI project and others did not contain DoD data. For those projects, we selected the next project in the category. We followed this process until a suitable project was identified.

# Management Comments

## U.S. Army



Office, Chief Information Officer/G-6

**DEPARTMENT OF THE ARMY**  
OFFICE OF THE SECRETARY OF THE ARMY  
107 ARMY PENTAGON  
WASHINGTON, DC 20310-0107

SAIS-CBA

MEMORANDUM FOR Department of Defense Office of Inspector General (DoDIG),  
4800 Mark Center Drive, Alexandria, VA 22350-1500

SUBJECT: Headquarters Department of the Army (HQDA) Chief Information Officer (CIO)/G-6 Response to the Department of Defense Office of Inspector General's Draft Report on the Governance and Protection of Department of Defense Artificial Intelligence Data and Technology (D2019-D000CR-0132.000)

1. Reference Memorandum, Department of Defense Inspector General, March 30, 2020, subject: Governance and Protection of Artificial Intelligence Data and Technology (D2019- D000CR-0132.000).
2. This memorandum and enclosure comprise the Army's position to the draft report for DoDIG Project Number D2019-D000CR-0132.000, "Governance and Protection of Artificial Intelligence Data and Technology."
3. We concur with DoDIG's recommendation that the Army develop and implement a plan to correct the weaknesses identified at facilities that manage artificial intelligence projects. The detailed response to the recommendation directed to the Army is included in the enclosure attached to this memorandum.
4. The point of contact for this memorandum is [REDACTED].

Encl

KREIDLER.NAN [REDACTED]  
CY [REDACTED]

NANCY KREIDLER  
Director, Cybersecurity and  
Information Assurance

## U.S. Army (cont'd)

The Army's Response to DoDIG's Recommendation in DoDIG Report, Governance and Protection of Artificial Intelligence Data and Technology, (D2019- D000CR-0132.000, dated March 30, 2020)

**Recommendation B1:** We recommend that the Chief Information Officers for the Army, Marine Corps, Navy, and Air Force develop and implement a plan to correct the weaknesses identified at facilities that manage artificial intelligence projects related to:

- a. Enforcing the use of multifactor authentication and strong passwords, when necessary, to reduce the risk of disclosing sensitive DoD information.
- b. Regularly monitoring networks and systems to identify unusual user and system activity.
- c. Configuring all systems to lock automatically after 15 minutes of inactivity.
- d. [REDACTED] to monitor personnel and respond to security incidents.
- e. Securing data centers, server racks, and associated keys.

**The Army's Response:** Concur. The subject report identified weaknesses at [REDACTED], which belongs to the Combat Capabilities Development Command (CCDC) C5ISR Center. The [REDACTED] discovered at [REDACTED] related to regularly monitoring unusual user activity and [REDACTED] to monitor personnel. CCDC provided a direct response to the DoDIG which included the C5ISR Center's actions taken to correct the weaknesses. The HQDA CIO/G-6 endorses the CCDC response. The Army has implemented policy in Army Regulation (AR) 25-2 (Cybersecurity), 4 April 2019, which addresses the identified weaknesses. Facilities that manage artificial intelligence projects are required to follow AR 25-2 which requires:

- a. The use of multifactor authentication and strong passwords.
- b. Commanders to monitor unusual activity as part of a comprehensive cybersecurity program.
- c. Following applicable STIGs which would include configuring all systems to lock automatically after 15 minutes of inactivity.
- d. The Provost Marshal General to ensure that the physical security program includes the measures required to safeguard information technology.
- e. Implementing the security controls from NIST 800-53 (Security and Privacy Controls for Federal Information Systems and Organizations).

## U.S. Army (cont'd)



DEPARTMENT OF THE ARMY  
U.S. ARMY COMBAT CAPABILITIES DEVELOPMENT COMMAND  
6662 GUNNER CIRCLE  
ABERDEEN PROVING GROUND, MARYLAND 21005-5201

FCDD-CG

27 April 2020

MEMORANDUM FOR Department of Defense Office of Inspector General, 4800 Mark Center Drive, Alexandria, VA 22350-1500

SUBJECT: U.S. Army Combat Capabilities Development Command Response to the Department of Defense Office of Inspector General's Draft Report on the Governance and Protection of Department of Defense Artificial Intelligence Data and Technology (D2019-D000CR-0132.000)

1. The Department of Defense Office of Inspector General (DoDIG) conducted an audit of DoD's governance and protection of Artificial Intelligence (AI) data. The objective was to determine the DoD's progress in developing an AI governance framework and to determine whether the DoD implemented security mechanisms to protect AI from cyber threats. The Combat Capabilities Development Command Internal Review (CCDC IR) Office has reviewed the results and recommendations of the audit engagement.
2. The DoDIG provided a five-part recommendation to the Chief Information Officer (CIO) at the services; however, only two of the five parts were found at the Army. During the audit engagement, the only Army organization visited by the DoDIG was the [REDACTED], which belongs to the CCDC C5ISR Center. As a result, CCDC is providing a response to the findings.
3. The DoDIG recommended that the Army develop and implement a plan to correct the weaknesses identified at facilities that manage artificial intelligence projects. The [REDACTED] related to [REDACTED] CCDC C5ISR concurs with the recommendation; however, corrective action had taken place before audit fieldwork had ended. We provided information to the DoDIG in October 2019.
4. While CCDC does concur with the recommendations, it should be noted that the [REDACTED] project may not be representative of the entire Army. During the audit, we informed DoDIG that the C5ISR Center facility visited was not currently processing either classified or controlled/sensitive unclassified data in the AI project identified. As such, many of the security protocols that would need to be in place are not required until CCDC starts processing or storing classified AI data. DoDIG acknowledged this and during the site visit exit briefing, DoDIG informed CCDC that these areas would only be items of consideration and not findings until the facility processed classified data. In addition, this particular AI project consists of only 5.5 FTEs and one 1.5 FTE for System Administration/Information Assurance support.

## U.S. Army (cont'd)

FCDD-CG

SUBJECT: U.S. Army Combat Capabilities Development Command Response to the Department of Defense Office of Inspector General's Draft Report on the Governance and Protection of Department of Defense Artificial Intelligence Data and Technology (D2019-D000CR-0132.000)

5. The CCDC endorses the detailed response by CCDC C5ISR, included as an enclosure to this memorandum.

6. The POC for this action is [REDACTED]

Encl  
CCDC C5ISR Response

GEORGE.JOHN.AN  
DERSON.SR. [REDACTED]

[REDACTED]  
JOHN A. GEORGE  
Major General, U.S. Army  
Commanding

# U.S. Army (cont'd)



UNCLASSIFIED//FOR OFFICIAL USE ONLY

**DEPARTMENT OF THE ARMY**  
U.S. ARMY COMBAT CAPABILITIES DEVELOPMENT COMMAND  
C5ISR CENTER  
6585 SURVEILLANCE LOOP, BUILDING 6002  
ABERDEEN PROVING GROUND, MARYLAND 21005-1845

FCDD-ISD-D

24-Apr-2020

MEMORANDUM FOR Commanding General, U.S. Army Combat Capabilities Development Command (FCDD-CG/MG George), 6662 Gunner Circle, Aberdeen Proving Ground, MD 21005-5201

SUBJECT: U.S. Army Combat Capabilities Development Command Response to the Department of Defense Office of Inspector General's Draft Report on the Governance and Protection of Department of Defense Artificial Intelligence Data and Technology (D2019-D000CR-0132.000)

1. ~~(U//FOUO)~~ The Department of Defense (DoD) Office of Inspector General (DoDIG) conducted an audit of DoD's governance, protection and ownership rights of Artificial Intelligence (AI) technology and data. The 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. The Combat Capabilities Development Command (CCDC) C5ISR Center has reviewed the results and recommendations of the audit engagement.

2. ~~(U//FOUO)~~ DoDIG provided multi-faceted recommendations to the services however; [REDACTED] For reference purposes, the C5ISR Center AI research element is identified in the report as

[REDACTED]

a. ~~(U//FOUO)~~ C5ISR Center concurs with recommendation B.1.b. The findings cited in [REDACTED] were resolved and demonstrated during the inspection.

[REDACTED]

b. ~~(U//FOUO)~~ As noted during the DoDIG site visit to the C5ISR Center and in the report, [REDACTED]

[REDACTED]

UNCLASSIFIED//FOR OFFICIAL USE ONLY



## U.S. Army (cont'd)

FCDD-ISD-D

SUBJECT: U.S. Army Combat Capabilities Development Command Response to the Department of Defense Office of Inspector General's Draft Report on the Governance and Protection of Department of Defense Artificial Intelligence Data and Technology (D2019-D000CR-0132.000)

c. (U//FOUO) C5ISR Center concurs with Recommendation B.1.d, and has resolved the finding cited in [REDACTED]

d. (U//FOUO) During the site visit, DoDIG noted that C5ISR Center had a [REDACTED] C5ISR Center believes this adequately meets the [REDACTED] recommendation B.1.d. as defined in the report.

3. (U//FOUO) The POCs for this action are: [REDACTED]

Encl  
Draft DoDIG Report

ONEILL.PATRI [REDACTED]  
CK.J. [REDACTED]  
[REDACTED]  
PATRICK J. O'NEILL  
Director

## U.S. Army (cont'd)



DEPARTMENT OF THE ARMY  
ARMY FUTURES COMMAND  
ARMY ARTIFICIAL INTELLIGENCE TASK FORCE  
10 40<sup>TH</sup> STREET  
PITTSBURGH, PA 15201

FCAI-DI

29 April 2020

MEMORANDUM FOR Department of Defense Office of Inspector General (DoDIG),  
4800 Mark Center Drive, Alexandria, VA 22350-1500

SUBJECT: U.S. Army Combat Capabilities Development Command (CCDC) Response to the DoDIG's Draft Report on the Governance and Protection of Department of Defense (DoD) Artificial Intelligence (AI) Data and Technology (D2019-D000CR-0132.000)

1. The DoDIG conducted an audit of DoD's governance and protection of AI data. The objective was to determine the DoD's progress in developing an AI governance framework and to determine whether the DoD implemented security mechanisms to protect AI from cyber threats. While the DoDIG did not directly audit an Army AI Task Force (A-AI TF) project, the A-AI TF would like to provide some additional recommendations.
2. Many of the specific Army findings are traditional cyber, information technology, and physical security measures governed under Army Regulations, i.e., AR 25-1 (Army Information Technology), AR 25-2 (Army Cybersecurity), AR 190-13 (The Army Physical Security Program), and AR 380-5 (Army Information Security Program). The A-AI TF recommends that the Joint AI Center provide overarching guidance to the services, giving unity and urgency across the DoD. In addition, guidance from national level governing bodies such as NIST should be, at a minimum, consulted.
3. However, one-sized-fits-all policy is not appropriate for collecting, managing, and sharing AI and Machine Learning (AI/ML) data or the resultant AI/ML models. We need a spectrum of approaches to protect AI/ML data and technology that are appropriate for the system being protected from Distribution A (Fully Releasable) to highly classified (whose data and models inherent the same protection measures as the program's classification level). Different measures should apply for Army sponsored university partners than deployed operational systems supporting targeting. Furthermore, as data is stored and processed in commercial cloud environments, appropriate control measures need to be in place and assessed and, in particular, remote access to data.
4. Governance organizations should also acknowledge and develop protections for specific vulnerabilities of AI/ML systems that do not exist in regular information technology systems.
  - a. First, ML systems are by definition dynamic where the machine learns a pattern, condition, or behavior over time and updates its model based upon new information.

## U.S. Army (cont'd)

SUBJECT: Army Response to DoDIG AI Governance and Protection of DoD AI Data and Technology Draft Report (D2019-D000CR-0132.000)

This makes these systems adaptable, but vulnerable to degraded performance or even adversarial attacks where data may be injected into the system attempting to spoof a result or containment a training set. See "DeepSec"<sup>1</sup> for a list of adversarial attack examples. However, adversarial attacks typically require access to the model for repeated exploration that may not be a reasonable security concern in some situations.

b. AI models themselves have to be protected as potential hackers can reverse engineer both vulnerabilities of the model as well as some aspects of the original training data.

c. For mission critical systems, the providence of the data and the model needs to be maintained throughout its lifecycle to include up to Critical Program Information (CPI). See DoDI 5220.39.

d. ML based AI systems also have security flaws due to the characteristic that they are not perfectly determinate systems. The behavior of these systems cannot be predicted in every scenario. This creates a gap for exploitation, degradation, or destruction of systems that rely on such technology.

e. Furthermore, as more undeclared dependencies may exist in data being used in an AI system and create unintended bias<sup>2</sup>, it is critical that the use of data is tracked. The Army plans to develop an Enterprise Data Service Catalog [REDACTED] to track Army data and its use in analytics.

f. Finally, Operational Security (OPSEC, AR 530-1) should be updated to include the concept of counter AI, actions that friendly forces take to protect data their formations generate and inadvertently release to opposing AI collection activities.

5. The point of contact for this action is the undersigned at [REDACTED] or [REDACTED].

EASLEY.MATTHE [REDACTED]  
W.P. [REDACTED]  
MATTHEW P. EASLEY  
Brigadier General  
Director, Army AI Task Force

2 Encls  
1. DeepSec Article  
2. AI Bias Article

<sup>1</sup> "DeepSec: A Uniform Platform for Security Analysis of Deep Learning Models", Xiang Ling et al., 2019 *IEEE Symposium on Security and Privacy*, 19-23 May 2019, San Francisco, CA.

<sup>2</sup> "This is how AI bias really happens—and why it's so hard to fix", Karen Hao, *MIT Technology Review*, 04 Feb 2019

## U.S. Marine Corps



DEPARTMENT OF THE NAVY  
HEADQUARTERS UNITED STATES MARINE CORPS  
3000 MARINE CORPS PENTAGON  
WASHINGTON DC 20350-3000

IN REPLY REFER TO:  
2000  
DC I  
MAY 28 2020

From: Deputy Commandant for Information  
To: Department of Defense Inspector General (DODIG)

Subj: UNITED STATES MARINE CORPS RESPONSE TO GOVERNANCE AND  
PROTECTION OF DEPARTMENT OF DEFENSE ARTIFICIAL INTELLIGENCE  
DATA AND TECHNOLOGY (PROJECT NO. D2019-D000CR-0132.00) REPORT

Ref: (a) Draft Report on Governance and Protection of Department of Defense Artificial  
Intelligence (AI) Data and Technology (Project No. D2019-D000CR-0132.000)

Encl: (1) Marine Corps Responses to DODIG AI Audit Recommendations  
(2) Marine Corps Comment Review Matrix for Draft AI Audit Report  
(3) Marine Corps Security Marking Review for Draft AI Audit Report

1. In response to reference (a), the Marine Corps has conducted recommendations and public release reviews. Comments resulting from those reviews are attached in enclosures (1) to (3).

2. The HQMC DC I point of contact for this effort is [REDACTED]

A handwritten signature in black ink, appearing to read "L. E. Reynolds".

L. E. REYNOLDS  
LtGen, USMC

## U.S. Marine Corps (cont'd)

**DODIG DRAFT REPORT DATED MARCH 30, 2020  
PROJECT NO. D2019-D000CR-0132.000**

**“GOVERNANCE AND PROTECTION OF DEPARTMENT OF DEFENSE ARTIFICIAL  
INTELLIGENCE DATA AND TECHNOLOGY”**

**UNITED STATES MARINE CORPS COMMENTS  
TO THE DODIG RECOMMENDATION**

DODIG recommends that the Chief Information Officers for the Army, Marine Corps, Navy, and Air Force develop and implement a plan to correct the weaknesses identified at facilities that manage artificial intelligence projects related to:

**RECOMMENDATION B.1.a:** Enforcing the use of multifactor authentication and strong passwords, when necessary, to reduce the risk of disclosing sensitive DoD information.

**USMC RESPONSE:** The Marine Corps agrees with this recommendation and enforces the use of multifactor authentication in accordance with DoDI 8520.03 “Identity Authentication for Information Systems,” DODI 8520.02 “Public Key Infrastructure (PKI) and Public Key (PK) Enabling,” MCO 5239.2b “Marine Corps Cybersecurity,” and the “Marine Corps Enterprise Cybersecurity Manual (ECSM) 013 Public Key Infrastructure.” Waivers for the use of multifactor authentication are reviewed by the Authorizing Official (AO) on a case by case basis. In the event a system cannot support the use of multifactor authentication due to technical or operational constraints, the use of complex passwords is required (per the Marine Corps ECSM 007 Resource Access Guide).

In the case of the audited Marine Corps Directorate of Analytics & Performance Optimization (MCDAPO) [REDACTED], the system administrator took action to ensure that access to this closed network via laptops required input of strong passwords. In addition, there was a PKI waiver in place under the system’s authority to operate (ATO).

Overall, the effectiveness of cybersecurity programs, policies, and procedures are reviewed by means of established procedures to include DC I, IC4/ICC monthly security evaluations, Marine Corps Institutional Cybersecurity Enterprise Defense Evaluation Monitoring Team (ICE DEMon/White Teams) assessments, and Command Cyber Readiness Inspections (CCRIs). Following such assessments, appropriate corrective action is taken if vulnerabilities or non-compliance is found. Special attention will be put toward ensuring multifactor authentication and/or strong password requirements are complied with in upcoming cybersecurity assessments.

**RECOMMENDATION B.1.b:** Regularly monitoring networks and systems to identify unusual user and system activity.

**USMC RESPONSE:** The Marine Corps agrees with the recommendation. Per MCO 5239.2b, Marine Corps networks are continuously monitored with the use of intrusion detection and prevention systems (IDS/IPS). In addition, per MCO 5239.2b and ECSM 007, system and

## U.S. Marine Corps (cont'd)

network administrators reporting to their command ISSMs/ISSOs are responsible for monitoring user account and system activity, analyzing patterns of non-compliance or unauthorized activity, and for taking appropriate administrative or programmatic actions to minimize security risks and insider threats.

In the case of the audited Marine Corps Directorate of Analytics & Performance Optimization (MCDAPO) [REDACTED], the system administrator took action to ensure [REDACTED] occurs and that the times individuals access the system are recorded in logs. Furthermore, application logs are maintained for users whose accounts are locked due to exceeding log in attempts. Users who have been “locked out” must be reset by the administrator (no automatic re-enabling after a set time period expires is implemented).

As noted in the response to Recommendation B.1.a, the Marine Corps will also ensure special attention is put toward ensuring all networks and systems are monitored to identify unusual user and system activity during upcoming cybersecurity assessments.

**RECOMMENDATION B.1.c:** Configuring all systems to lock automatically after 15 minutes of inactivity.

**USMC RESPONSE:** The Marine Corps agrees with the recommendation. Account lockout is enforced via Group Policy Orchestrator (GPO) update. MCO 5239.2b requires that ISSM/ISSOs comply with DISA STIGs. DISA STIGS require lock out after periods of inactivity for the various operating systems used.

In the case of the audited Marine Corps Directorate of Analytics & Performance Optimization (MCDAPO) [REDACTED], this recommendation was complied with at the time of the audit.

As noted in the response to Recommendation B.1.a, the Marine Corps will also ensure special attention is put toward ensuring all systems lock automatically after 15 minutes of inactivity in upcoming cybersecurity assessments.

**RECOMMENDATION B.1.d:** [REDACTED] to monitor personnel and respond to security incidents.

**USMC RESPONSE:** The Marine Corps agrees with the recommendation. Marine Corps CEDCs have implemented appropriate physical security measures commensurate with applicable NIST SP 800-53 controls, to include [REDACTED]. The MCO 5239.2b and the Marine Corps EC5M 018 Marine Corps Assessment and Authorization Process (MCCAP) mandate compliance with the DODI 8510.01 Risk Management Framework (RMF) for DoD Information Technology (IT) which mandates implementing appropriate NIST SP 800-53 security controls corresponding to the categorization of the systems per CNSSI 1253.

In the case of the audited Marine Corps Directorate of Analytics & Performance Optimization (MCDAPO) [REDACTED], this recommendation was complied with at the time of the audit.

## U.S. Marine Corps (cont'd)

As noted in the response to Recommendation B.1.a, the Marine Corps will also ensure special attention is put toward ensuring facilities hosting IT systems have the appropriate physical security controls implemented based on their security categorization IAW the DODI 8510.01 in upcoming cybersecurity assessments.

**RECOMMENDATION B.1.e:** Securing data centers, server racks, and associated keys.

**USMC RESPONSE:** The Marine Corps agrees with the recommendation. Marine Corps CEDCs are secured via approved means such as badge-only access in accordance with applicable Federal, NIST, DON, and Marine Corps policies. Physical keys are secured in Federal approved safes/lockboxes. As described in the response to recommendation B.1.d, MCO 5239.2b and the Marine Corps ECSM 018 mandate compliance with the DODI 8510.01, which mandates implementing appropriate NIST SP 800-53 security controls (to include physical access controls) corresponding to the categorization of the systems per CNSSI 1253.

In the case of the audited Marine Corps Directorate of Analytics & Performance Optimization (MCDAPO) [REDACTED], the server room is within a SCIF. In addition, that server room requires CAC-enabled access via keypad and number combination. The master key to the room is locked in a safe when not used.

As noted in the responses to Recommendations B.1.a and B.1.d, the Marine Corps will also ensure special attention is put toward ensuring facilities hosting IT systems have the appropriate physical security controls implemented based on their security categorization IAW the DODI 8510.01 in upcoming cybersecurity assessments.

## U.S. Marine Corps (cont'd)

### STANDARDIZED COMMENT MATRIX PRIMER

The matrix below is a Word document table to be used as a template for submitting comments on draft publications and draft program directives. Except as noted below, an entry is required in each of the columns. To facilitate consolidating matrices from various sources, do not adjust the column widths. Use the column headings in the document header as a guide to adjust column widths.

#### Column 1 – ITEM

Numeric order of comments. Accomplish when all comments from all sources are entered and sorted. To number the matrix rows, highlight this column only and then select the numbering ICON on the formatting tool bar.

#### Column 2 – #

Used to track comments by source. Manually enter numbers from the first comment to the last comment. These numbers will stay with the comment and will not change when consolidated with other comments.

#### Column 3 – SOURCE

J1 - J-1	JFCOM - US Joint Forces Command
J2 - J-2	PACOM - US Pacific Command
J3 - J-3	SOCOM - US Special Operations Command
J4 - J-4	SOUTHCOM - US Southern Command
J5 - J-5	SPACECOM - US Space Command
J6 - J-6	STRATCOM - US Strategic Command
J7 - J-7	TRANSCOM - US Transportation Command
J8 - J-8	DTRA - Defense Threat Reduction Agency
USA - US Army	DIA - Defense Intelligence Agency
USN - US Navy	DLA - Defense Logistics Agency
USMC - US Marine Corps	MDO - Missile Defense Organization
USAF - US Air Force	NSA - National Security Agency
USCG - US Coast Guard	DISA - Defense Information Systems Agency
CENTCOM - US Central Command	NIMA - National Imagery and Mapping Agency
EUCOM - US European Command	LC - Joint Staff Office of Legal Counsel

#### Column 4 – TYPE

C – Critical (Contentious issue that will cause non-concurrence with publication)

M – Major (Incorrect material that may cause non-concurrence with publication)

S – Substantive (Factually incorrect material)

A – Administrative (grammar, punctuation, style, etc.)

#### Column 5 – PAGE

Page numbers expressed in decimal form using the following convention:  
(Page I-2 = 1.02, Page IV-56 = 4.56, etc.) Enables proper sorting.

0 – General Comments  
0.xx - Preface, TOC, Executive Summary (Page i = 0.01, Page XI = 0.11)  
1.xx – Chapter I  
2.xx – Chapter II  
3.xx – Chapter III  
x.xx – Chapter x, etc.  
51.xx – Appendix A  
52.xx – Appendix B  
52.01.xx - Annex A to Appendix B  
53.xx – Appendix C, etc.  
99.xx – Glossary

**NOTE:** For Program Directives enter the page number as a whole number, (1, 2, 3, etc.) PDs are normally sorted by paragraph and line number and the page number helps to find the paragraph.

#### Column 6 – PARA

Paragraph number that pertains to the comment expressed. (i.e. 4a, 6g, etc.)

**NOTE:** An entry in this column should be used when commenting on draft program directives. An entry is optional for comments on draft joint publications.

#### Column 7 – LINE

Line number on the designated page that pertains to the comment, expressed in decimal form (i.e., line 1=1, line 4-5 = 4.5, line 45-67 = 45.67, etc.) For figures where there is no line number, use "F" with the figure number expressed in decimal form (i.e. figure II-2 as line number F2.02). For appendices, use the "F" and the appendix letter with the figure number (i.e. appendix D, figure 13 as line number FD.13; appendix C, annex A, figure 7 as line number FCA.07)

#### Column 8 – COMMENT

Comment text in line-in-line-out format according to JSM 5711.01A, *Joint Staff Correspondence Preparation* (Examples are provided in JP 1-01, Annex A to Appendix E). To facilitate adjudication of comments, copy complete sentences into the matrix so that it may not be necessary to refer back to the publication to understand the rationale for the change. Do not use Tools, Track Changes mode to edit the comments in the matrix. Include deleted material in the comment in the strike through mode. Add material in the comment with underlining. Do not combine separate comments into one long comment in the matrix. (i.e. 5 comments rolled up into one).

#### Column 9 – RATIONALE

Provide concise objective explanation of the rationale for the comment.

#### Column 10 - DECISION

A – Accept

R – Reject (Rationale required for rejection.)

M - Accept with modification (Rationale required for modification.)

**NOTE:** This column is for the LA and JSDS use only. No rationale required for accepted items. Rationale for rejection is placed in the rationale comment box and highlighted for clarity. For modifications, the complete modified language will be placed (and annotated) as the bottom entry for that item in the "Comments" column and the rationale for the modification placed in the rationale comment box and highlighted for clarity.

#### TIPS AND TRICKS OF THE TRADE



## U.S. Marine Corps (cont'd)

### TIPS AND TRICKS OF THE TRADE

#### Headers and Footers

1. Publication name
2. Classification (Unclassified/Secret/ etc.)
3. Column headings
4. Filename (insert from header/footer drop down menu)
5. As of "date" (insert from header/footer drop down menu—manually enter date when finalized for tracking purposes)
6. Page X of Y (insert from header/footer drop down menu—manually enter last page number for Y when finalized—tracks total # of pages and does not default back to actual page #)

#### Combining Matrices

1. Select all and correct for font and font size (Times New Roman, #10).
2. Copy one entire matrix and paste it a few lines below the last row of another matrix.
3. Adjust column widths as necessary to match one matrix with the other (use the column headings in the document header as a guide).
4. Merge the matrices into one by deleting the lines between the two.

#### Item (row) numbering (automatic numbering)

1. Highlight column number 1 from top to bottom.
2. Delete the existing number and then renumber by selecting automatic line numbering on the formatting tool bar.

#### Sorting

1. Select: "Table" on top menu toolbar.
2. Select: "Sort."
3. Select: "Sort by, Column 5 (Page column), Number, Ascending."
4. Select: "Then by, Column 7 (Line column), Number, Ascending."
5. Select: "Then by, Column 4 (Type column), Text, Descending."

#### Executive Summaries

Do not make comments on the executive summary until the FC. Main body text will be copied and pasted into the executive summary reducing the amount of time spent on making the two accurate. The contractor with LA and/or JSDS input will include an executive summary in the FC released for review and comment.

## U.S. Marine Corps (cont'd)

Final  
Report Reference

### DODIG Draft Report, Proj. No. D2019-D000CR-0132.000 Governance and Protection of DOD AI Data and Technology

ITEM #	SOURCE	TYPE	PAGE	PARA	LINE	COMMENT	RATIONALE	RECOMMENDED CHANGE	DECISION (A/R/M)
1	DC I WRD	S	12	2		Paragraph 2, Sentence 3: Add the following to the beginning of the sentence "If technically feasible and a better use of fiscal resources"	The Services routinely coordinate with each other on projects and programs of record. When technically feasible we do partner with other services but currently not all projects and programs are visible accords all of the services.	If technically feasible and a better use of fiscal resources, 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	
2	USMC DC I, IC4/ICC [REDACTED]	S		ii and elsewhere in report too	Rt. column ; last one	There are 3 DoD Components, not 4 as the paragraph states.	DON is a DoD Component that is comprised of the Navy and the Marine Corps.	Change four DoD Components to: four Military Services  and anywhere else it exists in the report	
3	USMC DC I, IC4/ICC [REDACTED]	S		i and page 3	Rt. column ; 2nd to last one and last para pg 3	Dates conflict for DoD AI policy due date Page 1 says April 2020 Page 3 says Mar 2020	Should have same date for same deliverable in the doc (consistency)	Recommend making them consistent	
4	USMC DC I, IC4/ICC [REDACTED]	A	page 7	1st bullet		remove word "begins"	extra word which doesn't make sense	remove word "begins"	
5	USMC DC I, IC4/ICC [REDACTED]	S	page 14 and elsewhere in report too	2nd para		Marine Corps Force Preservation Directorate changed its name to Marine Corps Directorate of Analytics & Performance Optimization (MCDAPO)	Name change occurred in Sept 2019	Recommend changing all references to Marine Corps Force Preservation Directorate in the report to: Marine Corps Directorate of Analytics & Performance Optimization (MCDAPO)  and all MCPD references in the report to MCDAPO	

Page 15

# U.S. Navy



DEPARTMENT OF THE NAVY  
OFFICE OF THE CHIEF OF NAVAL OPERATIONS  
2000 NAVY PENTAGON  
WASHINGTON, DC 20350-2000

5000  
Ser N2N6/20U119047  
08 May 20

From: Deputy Chief of Naval Operations for Information Warfare (N2N6)  
To: Department of Defense, Inspector General

Subj: NAVY RESPONSE TO THE DEPARTMENT OF DEFENSE INSPECTOR GENERAL  
GOVERNANCE AND PROTECTION OF DEPARTMENT OF DEFENSE ARTIFICIAL  
INTELLIGENCE DATA AND TECHNOLOGY AUDIT REPORT

Ref: (a) DoDIG Project No. D2019-D000CR-0132.000 of 30 Mar 20

1. This memorandum provides the Navy response to reference (a), the draft Department of Defense (DoD) Inspector General (IG) report on the Governance and Protection of DoD Artificial Intelligence (AI) Data and Technology. We submit the below comments on the Finding A recommendations.

a. Recommendation A.1.a: A single AI definition risks being overly broad. Recommend categorizing into types or tiers based on the application or effect. If being used for oversight or funding purposes, recommend it includes sufficient details to assist services in identifying the correct definition.

b. Recommendation A.1.b: Navy concurs with needing a Security Classification Guide (SCG), but recommends developing in a manner that protects sensitive data and capabilities while preserving innovation. Also, recommend using the Joint Artificial Intelligence Center (JAIC) SCG as a baseline for developing mission-driven SCGs requiring additional protections.

c. Recommendation A.1.d: Navy recommends the JAIC maintain and publish a data ontology, in cooperation with the services, to facilitate maximum interoperability. AI projects requesting usage of the data within or inclusion in the central repository could be evaluated against the ontology for compliance.

3. Navy non-concurs with Finding B which states that Naval Information Warfare Center [REDACTED] (NIWC [REDACTED]) did not implement physical security controls to detect and prevent unauthorized access and was non-compliant with NIST SP 800-53 due to not having [REDACTED] installed.

a. NIWC [REDACTED] T assets have a security categorization level of Moderate (confidentiality) / Moderate (integrity) / Low (availability) based on the data type protected. Per NIST 800-53 (Rev. 4), only the PE-6(1) security control applies; PE-6(2) through PE-6(4) requiring [REDACTED] is only applicable to systems with a high security classification level. For NIWC [REDACTED] it is an enhancement for consideration; it is not a control baseline requirement.

b. NIST 800-53 (page F-5) states that organizations operating national security systems “can use the security controls and control enhancements on a voluntary basis”. Secretary of the Navy Instruction (SECNAVINST) 5500.35, Office of the Chief of Naval Operations Instruction (OPNAVINST) 5530.14, and DoD Instruction (DoDI) 8510.01 establish Navy requirements and not include the physical security enhancements in the NIST 800-53.

c. Based on DoD policy not requiring the NIST 800-53 physical security control enhancements and that NIST 800-53 [REDACTED] baselines are not required, Navy requests that the Finding B section “Physical Security Controls Were Not Used to Detect and Prevent Unauthorized Access” be updated to reflect compliance. As Navy contests the finding, we also request that Table 3 be updated and that Navy be removed from the verbiage of Recommendation B.1.

## U.S. Navy (cont'd)

Subj: NAVY RESPONSE TO THE DEPARTMENT OF DEFENSE INSPECTOR GENERAL  
GOVERNANCE AND PROTECTION OF DEPARTMENT OF DEFENSE ARTIFICIAL  
INTELLIGENCE DATA AND TECHNOLOGY AUDIT REPORT

4. Points of contact listed below:

- a. AI - [REDACTED]
- b. Physical Security - [REDACTED]
- c. Naval Information Warfare Systems Command (NAVWAR) - [REDACTED]
- d. Cybersecurity - [REDACTED]



MATTHEW J. KOHLER

Copy to:  
DON CIO  
NAVWAR CIO  
[REDACTED]

## U.S. Air Force



**DEPARTMENT OF THE AIR FORCE  
WASHINGTON, DC**

OFFICE OF THE ASSISTANT SECRETARY

29 April 2020

MEMORANDUM FOR DEPARTMENT OF DEFENSE INSPECTOR GENERAL

FROM: SAF/CN  
1800 Air Force Pentagon Suite 4E226  
Washington, DC 20330

SUBJECT: Air Force Response to DoD Office of Inspector General Draft Report, "Governance and Protection of Department of Defense Artificial Intelligence Data and Technology" (Project No. D2019-D000CR-0132.000)

1. This is the Department of the Air Force response to the DODIG Draft Report, "Governance and Protection of Department of Defense Artificial Intelligence Data and Technology" (Project No. D2019-D000CR-0132.000). The SAF/CN concurs with the report as written and welcomes the opportunity to address the applicable recommendations.
2. SAF/CN will correct issues identified in this report, and develop and implement a corrective action plan outlined in the following recommendations:

**RECOMMENDATION 1:** The DODIG recommends that the Air Force enforce the use of multifactor authentication and strong passwords, when necessary, to reduce the risk of disclosing sensitive DoD information.

**AIR FORCE RESPONSE:** The Air Force concurs with this recommendation. The security deficiencies listed in in this recommendation can be mitigated by properly following the NIST Special Publication 800-37, Guide for Applying the Risk Management Framework (RMF), which is required to accredit all AF information systems. SAF/CN will draft a memo to Department of the Air Force Authorizing Officials (AO) emphasizing the need to properly follow applicable security guidance in order to protect Artificial Intelligence systems. The memo will be published by 1 July 2020.

**RECOMMENDATION 2:** The DODIG recommends that the Air Force regularly monitor networks and systems to identify unusual user and system activity.

**AIR FORCE RESPONSE:** The Air Force concurs with this recommendation. The security deficiencies listed in in this recommendation can be mitigated by properly following the NIST Special Publication 800-37, Guide for Applying the Risk Management Framework (RMF), which is required to accredit all AF information systems. SAF/CN will draft a memo to Department of the Air Force AOs emphasizing the need to properly follow applicable security guidance in order to protect Artificial Intelligence systems. The memo will be published by 1 July 2020.

**RECOMMENDATION 3:** The DODIG recommends that the Air Force configure all systems to lock automatically after 15 minutes of activity.

## U.S. Air Force (cont'd)

**AIR FORCE RESPONSE:** The Air Force concurs with this recommendation. The security deficiencies listed in in this recommendation can be mitigated by properly following the NIST Special Publication 800-37, Guide for Applying the Risk Management Framework (RMF), which is required to accredit all AF information systems. SAF/CN will draft a memo to Department of the Air Force AOs emphasizing the need to properly follow applicable security guidance in order to protect Artificial Intelligence systems. The memo will be published by 1 July 2020.

**RECOMMENDATION 4:** The DODIG recommends that the Air Force [REDACTED].

**AIR FORCE RESPONSE:** The Air Force concurs with this recommendation. The security deficiencies listed in in this recommendation can be mitigated by properly following the NIST Special Publication 800-37, Guide for Applying the Risk Management Framework (RMF), which is required to accredit all AF information systems. SAF/CN will draft a memo to Department of the Air Force AOs emphasizing the need to properly follow applicable security guidance in order to protect Artificial Intelligence systems. The memo will be published by 1 July 2020.

**RECOMMENDATION 5:** The DODIG recommends that the Air Force secure data centers, server racks, and associated keys.

**AIR FORCE RESPONSE:** The Air Force concurs with this recommendation. The security deficiencies listed in in this recommendation can be mitigated by properly following the NIST Special Publication 800-37, Guide for Applying the Risk Management Framework (RMF), which is required to accredit all AF information systems. SAF/CN will draft a memo to Department of the Air Force AOs emphasizing the need to properly follow applicable security guidance in order to protect Artificial Intelligence systems. The memo will be published by 1 July 2020.

3. The SAF/DCIO point of contact is [REDACTED]  
or via email at [REDACTED]

HATCHER.ARTHUR.GE [REDACTED]  
ORGE.JR [REDACTED]

ARTHUR G. HATCHER, SES, USAF  
Associate Deputy Chief Information Officer

### Attachment

1. Security Marking Review
2. Congressional/Media Interest Items slide

# Joint Artificial Intelligence Center



CHIEF INFORMATION OFFICER

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

APR 28 2020

MEMORANDUM FOR INSPECTOR GENERAL OF THE DEPARTMENT OF DEFENSE

SUBJECT: Review and Comment of Department of Defense Inspector General Draft Audit Report "Governance and Protection of DoD Artificial Intelligence Data and Technology" (D2019-D000CR-312.000)

This is the DoD Chief Information Officer (CIO) response to the DoD Inspector General (IG) Draft Report, Governance and Protection of DoD Artificial Intelligence (AI) Data and Technology (D2019-D000CR-312.000).

**General Comments Recommendation A.1:**

Under "Finding A," the DoD CIO and the Joint Artificial Intelligence Center (JAIC) concur with four of seven recommendations and partially concur with three recommendations. While supportive of the IG's recommendations designed to strengthen DoD's AI-related governance and data protection, the final report does not completely reflect previous inputs to correct, clarify, or amplify applicable sections of the report.

The JAIC undertook a number of actions over the past year to enhance DoD-wide AI governance and to accelerate scaling AI and its impact across the Department. The JAIC will continue to coordinate AI governance on behalf of the Secretary of Defense and use the authorities delegated to Director, JAIC, pursuant to Section 238 of the FY2019 National Defense Authorization Act (NDAA) and through the Director, JAIC's designation as DoD's Senior Official for AI with principal responsibility for the coordination of activities relating to the development and demonstration of AI and machine learning (ML) for the Department. As part of these responsibilities, the JAIC provided an AI Implementation Plan to the Deputy Secretary of Defense. This plan sets out the responsibilities, goals, objectives, and processes for ensuring full implementation of the Department's AI Strategy, and responsible stewardship and synchronization of financial investments. The plan includes chartering a DoD AI Executive Steering Group (AI ESG), a DoD AI Working Group, and nine AI subcommittees focused in the following areas: AI workforce; technical standards; enterprise infrastructure; test and evaluation; acquisition, academia, and industry engagement; responsible AI; international engagement; intelligence and security; and intelligent automation.

**DoD IG RECOMMENDATION A.1.a:** We recommend that the Director, JAIC establish an AI governance framework that includes: A standard definition of artificial intelligence that is updated at least annually.

**DoD CIO/JAIC Response A.1.a:** Partially Agree.

The JAIC acknowledges the importance of ensuring a common lexicon in the area of AI, particularly when used to improve accounting for AI investments in a manner that helps Department leaders make informed strategy and resource decisions. However, the DoD AI ESG



## Joint Artificial Intelligence Center (cont'd)

agreed with the JAIC's recommendation in January 2019 to use the definition of AI within the 2018 DoD AI Strategy: "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." The Department of Defense's report "Posture for Artificial Intelligence," published in 2019 in response to FY2019 NDAA Section 238, noted the challenges associated with a single definition of AI. The report concluded that enforcing a DoD-wide definition of AI would likely be neither feasible nor helpful. Instead, the report emphasized the importance of identifying and tracking AI activities, investments, and programs. Moreover, changing the definition of AI annually would be counterproductive and would likely result in unnecessary major confusion across the Department. The IG's recommendation that the JAIC should update the Department's definition of AI on an annual basis does not align to any specific technical, operational, or programmatic requirement. The DoD AI ESG is best postured to determine whether and when the Department's definition should be updated.

**DoD IG RECOMMENDATION A.1.b:** We recommend that the Director, JAIC establish an AI governance framework that includes: A security classification guide to ensure consistent protection of data used and produced for AI projects.

**DoD CIO/JAIC Response A.1.b:** Partially Agree.

The DoD CIO/JAIC agrees with the importance of comprehensive AI security clearance guidance and with the imperative for data protection. The JAIC is currently developing a Security Classification Guide (SCG), incorporating the lessons learned from Project Maven's SCG developed in 2017 under the Under Secretary of Defense for Intelligence. However, the JAIC recommends deletion of the words "used and" from Recommendation A.1.b and revising this recommendation to read: "A security classification guide to ensure consistent protection of data produced for AI projects." The JAIC's AI/ML projects rely on data from myriad organizations. The JAIC uses the data originator's classification parameters and, where applicable and appropriate, works with the data owner to downgrade data classification. When the JAIC receives stewardship of data, it will rely on data governance policies and cybersecurity protections to maintain compliance with existing laws, regulations, and policies. Additionally, the Secretary of Defense delegated to Director, JAIC, Original Classification Authority up to the TOP SECRET level. The JAIC will use this authority during development of classification guidance for AI technologies, though this guide will not apply to data originating from outside the JAIC (as it will retain its original classification unless explicitly modified as noted above).

**DoD IG RECOMMENDATION A.1.c:** We recommend that the Director, JAIC establish an AI governance framework that includes: A baseline inventory of artificial intelligence projects ongoing within the DoD.

**DoD CIO/JAIC Response A.1.c:** Agree. In 2019, the JAIC coordinated with Office of the Secretary of Defense (OSD) Cost Assessment and Program Evaluation (CAPE) on a Department-wide data call to establish a baseline inventory of ongoing DoD AI projects. This baseline inventory was verified by the 2019 report on DoD AI and further refined during the IG investigation. Additionally, the JAIC will establish a biannual AI portfolio review with all DoD Components, with the first review scheduled for mid-2020.



## Joint Artificial Intelligence Center (cont'd)

**DoD IG RECOMMENDATION A.1.d:** We recommend that the Director, JAIC establish an AI governance framework that includes: A process for identifying, monitoring, tracking, and reporting artificial intelligence projects, on a prescribed basis, that also requires the DoD Military Services and Components to validate the resulting list of AI projects for accuracy.

**DoD CIO/JAIC Response A.1.d:** Agree. In August 2019, the DoD CIO published fiscal guidance that requires DoD Components to report AI investments in the annual Information Technology/Cyberspace Activities budget exhibit. The JAIC will establish a biannual AI portfolio review with all DoD Components, with the first review scheduled for mid-2020.

**DoD IG RECOMMENDATION A.1.e:** We recommend that the Director, JAIC establish an AI governance framework that includes: A central repository for storing and sharing tools, data, policies, and procedures related to AI projects and technologies.

**DoD CIO/JAIC Response A.1.e:** Agree. The JAIC Joint Common Foundation (JCF) is designed to provide a central repository for storing and sharing tools, data, policies, and procedures related to AI projects and technologies. The JCF will be a collaborative environment at multiple classification levels that will accelerate the development, testing, validation, and fielding of AI capabilities by providing a repository for sharing source code, models, algorithms, and other artifacts, as well as access to leading-edge AI/ML tools, frameworks, and other shared resources, such as high performance computing centers, test networks/ranges, and government/commercial cloud services.

**DoD IG RECOMMENDATION A.1.f:** We recommend that the Director, JAIC establish an AI governance framework that includes: Standards for assessing legal and privacy considerations when developing and using AI data and technologies.

**DoD CIO/JAIC Response A.1.f:** Partially Agree. The DoD CIO/JAIC agrees with the importance of assessing legal and privacy considerations when developing and using AI data and technologies. However, there is no single standard that can be applied to legal and privacy consideration; every case is different, to varying degrees. Rather than developing standards, the JAIC recommends developing and following standard operating procedures and processes, in coordination with the appropriate legal counsel. The JAIC also wants to underscore the importance of responsible and ethical development and employment of AI technologies, as noted in the Secretary of Defense's February 21, 2020 memorandum, "Artificial Intelligence Principles for the Department of Defense." For these reasons, the JAIC recommends revising A.1.f. to read: "Standard operating procedures and processes, in coordination with the appropriate OSD offices, for assessing legal and privacy considerations when developing and using AI data and technologies; and guidance, recommendations, or policies for responsible and ethical development and use of AI data and technologies."


**DoD IG RECOMMENDATION A.1.g:** We recommend that the Director, JAIC establish an AI governance framework that includes: A strategy for identifying similar artificial intelligence projects and promoting the collaboration of artificial intelligence efforts across the DoD.

## Joint Artificial Intelligence Center (cont'd)

**DoD CIO/JAIC Response A.1.g:** Agree. The planned personnel growth of the JAIC in FY2021 will provide the resources required to improve visibility into Department-wide AI projects, enhance collaboration on AI efforts, and support eliminating duplicative or non-performing projects. The JAIC Missions Directorate focus on early and frequent interaction with users and Service program offices will also enhance DoD-wide crossflow. The DoD AI governance forums will improve insights into existing and proposed AI projects across the Department. The JAIC will establish a biannual AI portfolio review with all DoD Components, with the first review scheduled for mid-2020.

**DoD IG RECOMMENDATIONS B.1 and B.2:** These recommendations do not contain any findings for the DoD CIO and the JAIC. However, in response to your request for a security review, we highlighted sections of the report that should be marked as UNCLASSIFIED//FOR OFFICIAL USE ONLY. These sections provide details on specific vulnerabilities and limitations that should not be released publicly.

My point of contact for this matter is [REDACTED] He can be reached at [REDACTED]  
or [REDACTED]



Dana Deasy

## Defense Threat Reduction Agency



DEFENSE THREAT REDUCTION AGENCY  
8725 JOHN J. KINGMAN ROAD, STOP 6201  
FORT BELVOIR, VA 22060-6201

April 24, 2020

MEMORANDUM FOR MEMORANDUM FOR CYBERSPACE OPERATIONS  
DIRECTORATE, OFFICE OF INSPECTOR GENERAL (ATTN:  
[REDACTED])

SUBJECT: Follow-up on Draft Report for Audit of the Governance and Protection of the DoD's Artificial Intelligence Technology and Data (Project No. D2019-D000CR-0312.000)

Reference: Draft Report for Audit of the Governance and Protection of the DoD's Artificial Intelligence Technology and Data (Project No. D2019-D000CR-0312.000)

This is in response to the Draft Report for Audit of the Governance and Protection of the DoD's Artificial Intelligence Technology and Data (Project No. D2019-D000CR-0312.000). DTRA is responding to the recommendations that apply to the Agency program audited by the OIG: B.2.a, c, e, and g. The following is provided as an update:

**Recommendation B.2; a. and e.:** We recommend that contracting officers for the Defense Threat Reduction Agency and the Strategic Capabilities Office, in coordination with their DoD requiring activities, develop and implement a plan to verify that contractors correct the weaknesses identified in this report related to:

a. assessing whether the loss of confidentiality, integrity, or availability of DoD information could have a negative effect on organizational assets, and requiring contractors to use multifactor authentication or configuring its systems to meet the minimum DoD password length and complexity requirements;

e. using an automatic system lockout after inactivity;

**Management Update:** Based on verification by the contract COR, the contractor has begun implementation of multifactor authentication based on RSA tokens and has resolved the issue pertaining to automatic system lockout. With the implementation of RSA tokens, passwords are no longer required.

**Recommendation B.2.c:** We recommend that contracting officers for the Defense Threat Reduction Agency and the Strategic Capabilities Office, in coordination with their DoD requiring activities, develop and implement a plan to verify that contractors correct the weaknesses identified in this report related to:

c. identifying and mitigating vulnerabilities in a timely manner;

## Defense Threat Reduction Agency (cont'd)

**Management Update:** Based on verification from the contract COR, the contractor has taken action to address the findings. Scans of contractor network are run weekly, but the [REDACTED] were initially not included in those scans. The contractor has since set up accounts [REDACTED] so that they are now part of the scans. The contractor reviews the results of network scans manually. The contractor is on track for implementing NIST 800-171 IT security compliance this year.

**Recommendation B.2.g:** We recommend that contracting officers for the Defense Threat Reduction Agency and the Strategic Capabilities Office, in coordination with their DoD requiring activities, develop and implement a plan to verify that contractors correct the weaknesses identified in this report related to:

g. implementing physical security safeguards for [REDACTED], and associated keys.

**Management Update:** Based on verification from the contract COR, the contractor has added physical locks to the [REDACTED] in the [REDACTED].

Thank you for the opportunity to respond to the draft report. Additional comments are included in the attached DTRA Comments Resolution Matrix for your consideration. Also attached is a signed Security Marking Review form and marked-up version of the draft report.

My point of contact in this matter is [REDACTED] or [REDACTED]

4/27/2020

X 

Signed by: LAKE.VICTOR.ASA [REDACTED]

Victor A. Lake, Captain, U.S. Navy  
Chief, RD-OPI

**Attachments:**

1. Consolidated DTRA OIG CRM (23 April 2020)
2. DTRA Security Marking Review - DRAFT Governance and Protection of DoD AI Data and Tech (22 April 2020)
3. DRAFT Governance and Protection of DoD AI Data and Tech - March 30 2020 (DTRA FOUO Review)

## Defense Threat Reduction Agency (cont'd)

CLASSIFICATION

### STANDARDIZED COMMENT MATRIX PRIMER

The matrix below is a Word document table to be used as a template for submitting comments on draft publications and draft program directives. Except as noted below, an entry is required in each of the columns. To facilitate consolidating matrixes from various sources, do not adjust the column widths. Use the column headings in the document header as a guide to adjust column widths.

#### Column 1 – ITEM

Numeric order of comments. Accomplish when all comments from all sources are entered and sorted. To number the matrix rows, highlight this column only and then select the numbering ICON on the formatting tool bar.

#### Column 2 - #

Used to track comments by source. Manually enter numbers from the first comment to the last comment. These numbers will stay with the comment and will not change when consolidated with other comments.

#### Column 3 – SOURCE

J1 - J-1	JFCOM - US Joint Forces Command
J2 - J-2	PACOM - US Pacific Command
J3 - J-3	SOCOM - US Special Operations Command
J4 - J-4	SOUTHCOM - US Southern Command
J5 - J-5	SPACECOM - US Space Command
J6 - J-6	STRATCOM - US Strategic Command
J7 - J-7	TRANSCOM - US Transportation Command
J8 - J-8	DTRA – Defense Threat Reduction Agency
USA – US Army	DIA – Defense Intelligence Agency
USN – US Navy	DLA – Defense Logistics Agency
USMC – US Marine Corps	MDO – Missile Defense Organization
USAF – US Air Force	NSA – National Security Agency
USCG – US Coast Guard	DISA – Defense Information Systems Agency
CENTCOM - US Central Command	NIMA – National Imagery and Mapping Agency
EUCOM - US European Command	LC – Joint Staff Office of Legal Counsel

#### Column 4 – TYPE

- C – Critical (Content issue that will cause non-concurrence with publication)
- M – Major (Incorrect material that may cause non-concurrence with publication)
- S – Substantive (Factually incorrect material)
- A – Administrative (grammar, punctuation, style, etc.)

#### Column 5 – PAGE

Page numbers expressed in decimal form using the following convention: (Page 1-2 = 1.02, Page IV-56 = 4.56, etc.) Enables proper sorting.

- 0 – General Comments
- 0.xx - Preface, TOC, Executive Summary (Page i = 0.01, Page XI = 0.11)
- 1.xx – Chapter I
- 2.xx – Chapter II
- 3.xx – Chapter III
- x.xx – Chapter x, etc.
- 51.xx – Appendix A
- 52.xx – Appendix B
- 52.01.xx - Annex A to Appendix B
- 53.xx – Appendix C, etc.
- 99.xx – Glossary

**NOTE:** For Program Directives enter the page number as a whole number, (1, 2, 3, etc.) PDs are normally sorted by paragraph and line number and the page number helps to find the paragraph.

#### Column 6 – PARA

Paragraph number that pertains to the comment expressed. (i.e. 4a, 6g, etc.)

**NOTE:** An entry in this column should be used when commenting on draft program directives. An entry is optional for comments on draft joint publications.

#### Column 7 – LINE

Line number on the designated page that pertains to the comment, expressed in decimal form (i.e., line 1=1, line 4-5 = 4.5, line 45-67 = 45.67, etc.) For figures where there is no line number, use "F" with the figure number expressed in decimal form (i.e. figure II-2 as line number F2.02). For appendices, use the "F" and the appendix letter with the figure number (i.e appendix D, figure 13 as line number FD.13; appendix C, annex A, figure 7 as line number FCA.07)

#### Column 8 – COMMENT

Comment text in line-in-line-out format according to JSM 5711.01A, *Joint Staff Correspondence Preparation* (Examples are provided in JP 1-01, Annex A to Appendix E). To facilitate adjudication of comments, copy complete sentences into the matrix so that it may not be necessary to refer back to the publication to understand the rationale for the change. Do not use Tools, Track Changes mode to edit the comments in the matrix. Include deleted material in the comment in the strike through mode. Add material in the comment with underlining. Do not combine separate comments into one long comment in the matrix, (i.e. 5 comments rolled up into one).

## Defense Threat Reduction Agency (cont'd)

CLASSIFICATION

### Column 9 - RATIONALE

Provide concise objective explanation of the rationale for the comment.

### Column 10 - DECISION

A - Accept

R - Reject (Rationale required for rejection.)

M - Accept with modification (Rationale required for modification.)

**NOTE:** This column is for the LA and JSDS use only. No rationale required for accepted items. Rationale for rejection is placed in the rationale comment box and highlighted for clarity. For modifications, the complete modified language will be placed (and annotated) as the bottom entry for that item in the "Comments" column and the rationale for the modification placed in the rationale comment box and highlighted for clarity.

### TIPS AND TRICKS OF THE TRADE

#### Headers and Footers

1. Publication name
2. Classification (Unclassified/Secret/ etc.)
3. Column headings
4. Filename (insert from header/footer drop down menu)
5. As of "date" (insert from header/footer drop down menu—manually enter date when finalized for tracking purposes)
6. Page X of Y (insert from header/footer drop down menu—manually enter last page number for Y when finalized—tracks total # of pages and does not default back to actual page #)

#### Combining Matrixes

1. Select all and correct for font and font size (Times New Roman, #10).
2. Copy one entire matrix and paste it a few lines below the last row of another matrix.
3. Adjust column widths as necessary to match one matrix with the other (use the column headings in the document header as a guide).
4. Merge the matrices into one by deleting the lines between the two.

#### Item (row) numbering (automatic numbering)

1. Highlight column number 1 from top to bottom.
2. Delete the existing number and then renumber by selecting automatic line numbering on the formatting tool bar.

#### Sorting

1. Select: "Table" on top menu toolbar.
2. Select: "Sort."
3. Select: "Sort by, Column 5 (Page column), Number, Ascending."
4. Select: "Then by, Column 7 (Line column), Number, Ascending."
5. Select: "Then by, Column 4 (Type column), Text, Descending."

#### Executive Summaries

Do not make comments on the executive summary until the FC. Main body text will be copied and pasted into the executive summary reducing the amount of time spent on making the two accurate. The contractor with LA and/or JSDS input will include an executive summary in the FC released for review and comment.

## Defense Threat Reduction Agency (cont'd)

CLASSIFICATION

**Final  
Report Reference**

1.	2	DTRA AL (Contracts)	M	21, 23-24	B.2.a; e	N/A	<i>[As is] Recommendation B.2</i> We recommend that contracting officers for the Defense Threat Reduction Agency and the Strategic Capabilities Office, in coordination with their DoD requiring activities, develop and implement a plan to verify that contractors correct the weaknesses identified in this report related to: a. assessing whether the loss of confidentiality, integrity, or availability of DoD information could have a negative effect on organizational assets, and requiring contractors to use multifactor authentication or configuring its systems to meet the minimum DoD password length and complexity requirements; e. using an automatic system lockout after inactivity;	B.2.a and B.2.e: Concur - based on verification by the contract COR, the contractor has begun implementation of multifactor authentication based on RSA tokens and has resolved the issue pertaining to automatic system lockout. With the implementation of RSA tokens, passwords are no longer required.	
2.	3	DTRA AL (Contracts)	M	22	B.2.c	N/A	<i>[As is] Recommendation B.2</i> We recommend that contracting officers for the Defense Threat Reduction Agency and the Strategic Capabilities Office, in coordination with their DoD requiring activities, develop and implement a plan to verify that contractors correct the weaknesses identified in this report related to: c. identifying and mitigating vulnerabilities in a timely manner;	B.2.c: Concur - based on verification from the contract COR, the contractor has taken action to address the findings.	
3.	5	DTRA AL (Contracts)	M	25	B.2.f; g		<i>[As is] Recommendation B.2</i> We recommend that contracting officers for the Defense Threat Reduction Agency and the Strategic Capabilities Office, in coordination with their DoD requiring activities, develop and implement a plan to verify that contractors correct the weaknesses identified in this report related to: g. implementing physical security safeguards for [REDACTED]	B.2.g: Concur – based on verification from the contract COR, the contractor has added [REDACTED]	
4.	1	DTRA RD- CX (AWeS PM)	M	20	N/A	3	<i>[As is] (Recommendation A.1.a) The JAIC should develop a standard definition of AI.</i>  <del>(U//FOUO)</del> Recommend a tiered definition of AI and a commensurate system of security requirements, which allow users/developers the flexibility to work on simple or complex AI tasks and safeguard that information accordingly. This would be a “Tiered” approach to security.	<del>(U//FOUO)</del> A standard definition of AI could require all security standards be implemented regardless of the scale and type of AI research.  However, if there were a tiered definition, contractors would be able to meet the security standards for their level of AI research and not implement the full measure of security standards	

**Page 46**

**Page 48**

**Page 51**

**Page 18**

## Defense Threat Reduction Agency (cont'd)

CLASSIFICATION

**Final  
Report Reference**

									if not applicable to the specific scale or type on investment.
5.	2	DTRA RD-CXS (AWeS PM)	M	20-21, 23	B.2.a; e	N/A	<p><i>[As is] Recommendation B.2</i> We recommend that contracting officers for the Defense Threat Reduction Agency and the Strategic Capabilities Office, in coordination with their DoD requiring activities, develop and implement a plan to verify that contractors correct the weaknesses identified in this report related to:</p> <p>a. assessing whether the loss of confidentiality, integrity, or availability of DoD information could have a negative effect on organizational assets, and requiring contractors to use multifactor authentication or configuring its systems to meet the minimum DoD password length and complexity requirements;</p> <p>e. using an automatic system lockout after inactivity;</p>	<p>Recommendation B.2.a and B.2.e refer specifically to a few ██████████ used for machine learning computations. The DTRA contractor has implemented multifactor authentication based on RSA tokens on those systems since the original audit. The contractor has successfully configured one of the systems. The others should be complete soon. The inactivity lock has also been resolved. With the implementation of RSA tokens, passwords are no longer required. The PIN + rotating fob value is the password and address requirements.</p>	
6.	3	DTRA RD-CXS (AWeS PM)	M	22	B.2.b; c	N/A	<p><i>[As is] Recommendation B.2</i> We recommend that contracting officers for the Defense Threat Reduction Agency and the Strategic Capabilities Office, in coordination with their DoD requiring activities, develop and implement a plan to verify that contractors correct the weaknesses identified in this report related to:</p> <p>c. identifying and mitigating vulnerabilities in a timely manner;</p>	<p>Scans of contractor network are run weekly, though the ██████████ were not initially included in those scans. The contractor has since set up accounts ██████████ so that they are now part of the scans. The contractor reviews the results of network scans manually. The contractor is on track for implementing NIST 800-171 IT security compliance this year.</p>	
7.	5	DTRA RD-CXS (AWeS PM)	M	25-26	B.2.f; g		<p><i>[As is] Recommendation B.2</i> We recommend that contracting officers for the Defense Threat Reduction Agency and the Strategic Capabilities Office, in coordination with their DoD requiring activities, develop and implement a plan to verify that contractors correct the weaknesses identified in this report related to:</p> <p>g. implementing physical security safeguards for ██████████, and associated keys.</p>	<p>All ██████████ are currently operated in ██████████ only accessible by authorized personnel. The contractor has added ██████████ in the ██████████. The OIG's concern was an insider</p>	

**Page 46**

**Page 48**

**Page 51**



## Defense Threat Reduction Agency (cont'd)

CLASSIFICATION

**Final  
Report Reference**

								threat having access to drives and hardware.	
8.	1	DTRA IT	C	21	2	10-13	I don't believe it is typically within the skillset of the contracting officer to be able to assess what impact the loss of specific data would have to the organization. I believe an assessment of this type would be more accurate if provided by the program manager of the contract or the contracting officer technical representative. There should be some sort of caveat or requirement statement within all off-site DTRA contracts containing information technology assets not under DTRA control stating compliance with NIST 800-171 is required. PMs can track their compliance if a plan of action and milestones is required as a deliverable for any NIST 800-171 non-compliance items.	The contracting officer will not have the knowledge of all data points produced within a particular contract. This would be more in the PM's realm with assistance of the COTR and perhaps the OPSEC team from Security and Counterintelligence. PM and COTR will have the most knowledge of any IT systems operated by contractors under contracts for DTRA and would have more access to validate compliance. It is not within the scope of DTRA Cyber Security nor are they resourced to evaluate systems located at vendor sites for all DTRA contracts.	
9.	2	DTRA IT	C	22	1	15-18	This should be a PM/COTR responsibility. NIST 800-17 requires vulnerability scanning to be accomplished. The contracting officer could assist by ensuring NIST 800-171 compliance and POAM deliverable caveats are added to all DTRA contracts containing information technology assets not under DTRA control.	PM/COTR will be more knowledgeable on specifics than the contracting officer would be and should track compliance with a POAM. It is not within the scope of DTRA Cyber Security nor are they resourced to evaluate systems located at vendor sites for all DTRA contracts.	
10.	3	DTRA IT	C	23	4	8	This should be a PM/COTR responsibility. NIST 800-17 requires session lockout after a period on non-activity, although it doesn't state a specific length of time. Although they are not required to use the DoD Security Technical Implementation Guides (STIG) it is a safe way to meet compliance. The contracting officer could assist by ensuring NIST 800-171 compliance and POAM deliverable caveats are added to all DTRA contracts containing information technology assets not under DTRA control.	PM/COTR will be more knowledgeable on specifics than the contracting officer would be and should track compliance with a POAM. It is not within the scope of DTRA Cyber Security nor are they resourced to evaluate systems located at vendor sites for all DTRA contracts.	
11.	4	DTRA IT	C	25	2	11-14	This should be a PM/COTR responsibility. NIST 800-53 requires [REDACTED] to be in [REDACTED]. This could cause unauthorized personnel to have access to sensitive data. The contracting officer could assist by ensuring NIST 800-53 compliance and [REDACTED] a	PM/COTR should track compliance with this. Ensure access restrictions are enforced to the [REDACTED] and if [REDACTED], a	

**Page 46**

**Page 48**

**Page 49**

**Page 51**

## Defense Threat Reduction Agency (cont'd)

CLASSIFICATION

**Final  
Report Reference**

							POAM deliverable caveats are added to all DTRA contracts containing information technology assets/facilities not under DTRA control.	POAM should be created. It is not within the scope of DTRA Physical Security nor are they resourced to evaluate vendor facilities for all DTRA contracts	
12.	1	DTRA OI (Security)	S	25	B.1.e and B.2.g		In response to recommendations B.1.e and B.2.g, The DTRA Program Protection Office will work with the DTRA AI Program manager and tech integrators to complete a program review and establish a Program Protection Plan (PPP) as warranted. The PPP will consist of Intel/CI Threat Assessment, SCRM Assessment, HW/SW Assurance, Cyber Security Strategy, OPSEC Plan, PHYSEC requirements and Security Classification Guides. These documents will inform the PM of the threats, identify risk, and provide countermeasures to reduce the risk to the effort. In addition, the Program Protection Office will coordinate with other services and agencies to conduct horizontal protection as required by DOD policy. The DTRA Program Protection Office in OI-MSCS will work with the DTRA AI Program manager to complete a program review and establish Program Protection Plan as warranted. The Program Protection Plan will consist of OPSEC, PHYSEC and INFOSEC Plans.	DTRA response to B.1.e and B.2.g recommendations.	

**Page 44**

## Strategic Capabilities Office



STRATEGIC  
CAPABILITIES OFFICE

OFFICE OF THE SECRETARY OF DEFENSE  
1000 DEFENSE PENTAGON  
WASHINGTON, DC 20301-1000

MEMORANDUM FOR DEPARTMENT OF DEFENSE, INSPECTOR GENERAL

FROM: Director, Strategic Capabilities Office

SUBJECT: Response to Department of Defense (DoD) Inspector General (IG) Draft Report for Audit of the Governance and Protection of the DoD's Artificial Intelligence Technology and Data (Project No. D2019-D000CR-0312.000)

1. This memorandum is in response to the March 30, 2020 DoD IG request for review and comment by the Strategic Capabilities Office (SCO) on the draft report for the subject audit. Specifically, the DoD IG lead auditor requested SCO's comments to recommendations B.2.b, B.2.d, and B.2.f. SCO is submitting this memorandum to provide clarification about SCO's authorities and to address formally the aforementioned recommendations.
2. In accordance with its chartering directive, DoD Directive 5105.86, *Director, Strategic Capabilities Office (SCO)*, dated November 14, 2016, SCO currently exercises "all necessary acquisition authorities through a Military Department, a DoD contract administration services component, or a federal department and agency, as appropriate, to further the SCO mission." SCO does not award or administer directly any contracting actions for its programs; thus, SCO is a requiring agency for purposes of the audited activity. SCO relies upon a federated team of acquisition offices to support its mission and project execution. SCO is currently reviewing options for obtaining contracting authority in the future in order to manage more efficiently its portfolio of prototyping projects. In this instance, the contract that was audited was awarded by the Department of the Interior, Interior Business Center.
3. The contractor reviewed during this audit is performing work for SCO pursuant to an "other transaction-prototype agreement", awarded under the provisions 10 U.S.C. §2371b, which is not a Federal Acquisition Regulations-based contract. In accordance with the terms of the agreement, SCO retains Cognizant Security Authority for the work being performed by the contractor in support of the agreement. Under this arrangement, SCO's Security and Program Protection Directorate provides oversight and directive guidance regarding the relevant security authorities associated with all aspects of program protection (e.g., information security, cybersecurity, physical security, etc.) rather than the agreement or contracting officer. SCO has coordinated this response with the supporting agreement officer as DoD IG requested, but acknowledges that the oversight for these security measures remains with SCO's program manager and its Security and Program Protection Directorate.
4. **Recommendation B.2.b:** "...the SCO contracting officer should develop and implement a plan to verify its contractors consistently scan networks, including subfolders, for viruses." **SCO concurs with the recommendation. SCO's Program Security Representatives will continue**

**Final  
Report Reference**

**Redirected  
Recommendation B.2**

## Strategic Capabilities Office (cont'd)

**to monitor and verify contractor compliance through participation in quarterly program reviews and spot checks to ensure contractors consistently scan networks, to include all subfolders, with anti-virus (AV) software.**

- a. This recommendation stems from the contractor's AV software not being able to provide verification that it was configured to scan all subfolders.
- b. Corrective action was taken on the spot to ensure AV software was configured properly to enable the contractor to confirm scanning of all subfolders. This action was logged and incorporated into the Standing Operating Procedures (SOP), and evidence was provided to the audit team reflecting AV scans included all subfolders. After ensuring the proper configuration the scan identified no abnormalities within all folders and subfolders.
- c. Since the audit, the SCO's program security representative participates with the program manager in the quarterly program reviews and conducts spot checks to ensure AV scans are conducted in accordance with the SOP.

**5. Recommendation B.2.d:** "The SCO contracting officer should develop and implement a plan to ensure contractors [REDACTED] to identify unusual user and system activity." **SCO concurs with this recommendation. SCO's Security and Program Protection Directorate will continue to ensure contractors supporting SCO AI projects incorporate [REDACTED] into program specific protection plans.**

- a. This recommendation stems from the contractor's inability to demonstrate effectively that local network user activity was [REDACTED] to identify unusual user and system activity.
- b. Corrective action was taken on the spot. The contractor is [REDACTED]. This is reflected in the SOP and was implemented immediately. User activity [REDACTED] UserID/PW and two-factor authentication. The contractor provided to the audit team a printout of all users and their associated rights on or about August 19, 2019. Additionally, the SOP was updated to ensure the network where information is hosted is regularly scanned for vulnerabilities and anomalous user behavior. Since the audit, the program security representative participates in the quarterly program reviews and conducts spot checks to ensure the corrective actions are still occurring. To date, post audit monitoring has identified zero abnormalities in the network and systems.

**6. Recommendation B.2.f:** [REDACTED] **SCO non-concurs with this recommendation.**

- a. This recommendation stems from the auditor's observations related [REDACTED], specifically, the absence of [REDACTED]

## Strategic Capabilities Office (cont'd)

- [REDACTED]
- b. [REDACTED] is not a requirement per NIST 800-53 Rev4. During SCO's security site survey, it was determined that the [REDACTED] in place sufficiently satisfied program security requirements. The work site has security-in-depth via [REDACTED], roving security, a 24/7 on site security monitoring station monitored by security personnel who are vetted, U.S. citizens. These security personnel are dedicated to responding to any alarms or indications of forced entry. Local law enforcement are also present onsite. Badge readers on external and internal doors log access by individual. The [REDACTED] are located behind double-locked doors that require badge and physical key to access. Given this enhanced security posture, SCO's Security and Program Protection Directorate determined it was not fiscally prudent to require the contractor to [REDACTED]. SCO's program security representative assessed that the security-in-depth measures already in place at the site addressed the security of the [REDACTED]. Additionally, the program manager and program security representative have ensured visitor badges and logs are on site and being used to track all visitors.

7. The Points of Contact for this matter are [REDACTED]

or [REDACTED]

DRYER.JAY.EDW / [REDACTED]  
ARD [REDACTED]

Jay E. Dryer  
Director  
Strategic Capabilities Office

## Acronyms and Abbreviations

---

<b>AFRL</b>	Air Force Research Laboratory
<b>AI</b>	Artificial Intelligence
<b>CAPE</b>	Cost Assessment and Program Evaluation
<b>CIO</b>	Chief Information Officer
<b>DISA</b>	Defense Information Systems Agency
<b>DTRA</b>	Defense Threat Reduction Agency
<b>GAO</b>	Government Accountability Office
<b>JAIC</b>	Joint Artificial Intelligence Center
<b>MCDAPO</b>	Marine Corps Directorate of Analytics and Performance Optimization
<b>NDAA</b>	National Defense Authorization Act
<b>NIST</b>	National Institute of Standards and Technology
<b>NMI</b>	National Mission Initiative
<b>OIG</b>	Office of Inspector General
<b>SCO</b>	Strategic Capabilities Office
<b>SP</b>	Special Publication
<b>STIG</b>	Security Technical Implementation Guide

## Glossary

---

**Artificial Intelligence.** The ability of machines to perform tasks that normally require human intelligence whether digitally or as smart software behind autonomous physical systems.

**Artificial Intelligence Portfolio.** A complete and accurate listing of DoD AI projects with the governance and protection of AI data and technologies.

**Cyber Attack.** An attack, via cyberspace, targeting an enterprise's use of cyberspace for the purpose of disrupting, disabling, destroying, or maliciously controlling a computing environment or infrastructure, destroying the integrity of the data, or stealing controlled information.

**Malicious Activity.** Activities that seek to compromise or impair the confidentiality, integrity, or availability of computers, information or communications systems, networks, physical or virtual infrastructure controlled by computers or information systems, or information resident thereon.

**Multifactor Authentication.** Authentication using two or more different factors to achieve authentication. Factors include something you know (for example, personal identification number or password), something you have (for example, cryptographic identification device or token), or something you are (for example, biometric).

**National Mission Initiatives.** Large-scale efforts to apply AI as a solution to closely related and urgent challenges the DoD may encounter.

**Phishing.** A method malicious actors use to masquerade as a reputable entity or person to obtain sensitive information, such as passwords and financial information.

**Reverse Engineering.** The duplication of another product by thorough examination to understand how the product works, and enhance or duplicate the product

**Safeguards.** Protective measures prescribed to meet the security requirements (for example, confidentiality, integrity, and availability) specified for an information system. Safeguards may include security features, management constraints, personnel security, and security of physical structures, areas, and devices.

**Security Classification Guide.** The written record of an original classification decision or series of decisions regarding a system, plan, program, project, or mission.





## **Whistleblower Protection**

### **U.S. DEPARTMENT OF DEFENSE**

*Whistleblower Protection safeguards DoD employees against retaliation for protected disclosures that expose possible waste, fraud, and abuse in government programs. For more information, please visit the Whistleblower webpage at <http://www.dodig.mil/Components/Administrative-Investigations/Whistleblower-Reprisal-Investigations/Whistleblower-Reprisal/> or contact the Whistleblower Protection Coordinator at [Whistleblowerprotectioncoordinator@dodig.mil](mailto:Whistleblowerprotectioncoordinator@dodig.mil)*

## **For more information about DoD OIG reports or activities, please contact us:**

### **Congressional Liaison**

703.604.8324

### **Media Contact**

[public.affairs@dodig.mil](mailto:public.affairs@dodig.mil); 703.604.8324

### **DoD OIG Mailing Lists**

[www.dodig.mil/Mailing-Lists/](http://www.dodig.mil/Mailing-Lists/)

### **Twitter**

[www.twitter.com/DoD\\_IG](http://www.twitter.com/DoD_IG)

### **DoD Hotline**

[www.dodig.mil/hotline](http://www.dodig.mil/hotline)

~~FOR OFFICIAL USE ONLY~~



DEPARTMENT OF DEFENSE | OFFICE OF INSPECTOR GENERAL

4800 Mark Center Drive  
Alexandria, Virginia 22350-1500  
[www.dodig.mil](http://www.dodig.mil)  
DoD Hotline 1.800.424.9098

~~FOR OFFICIAL USE ONLY~~