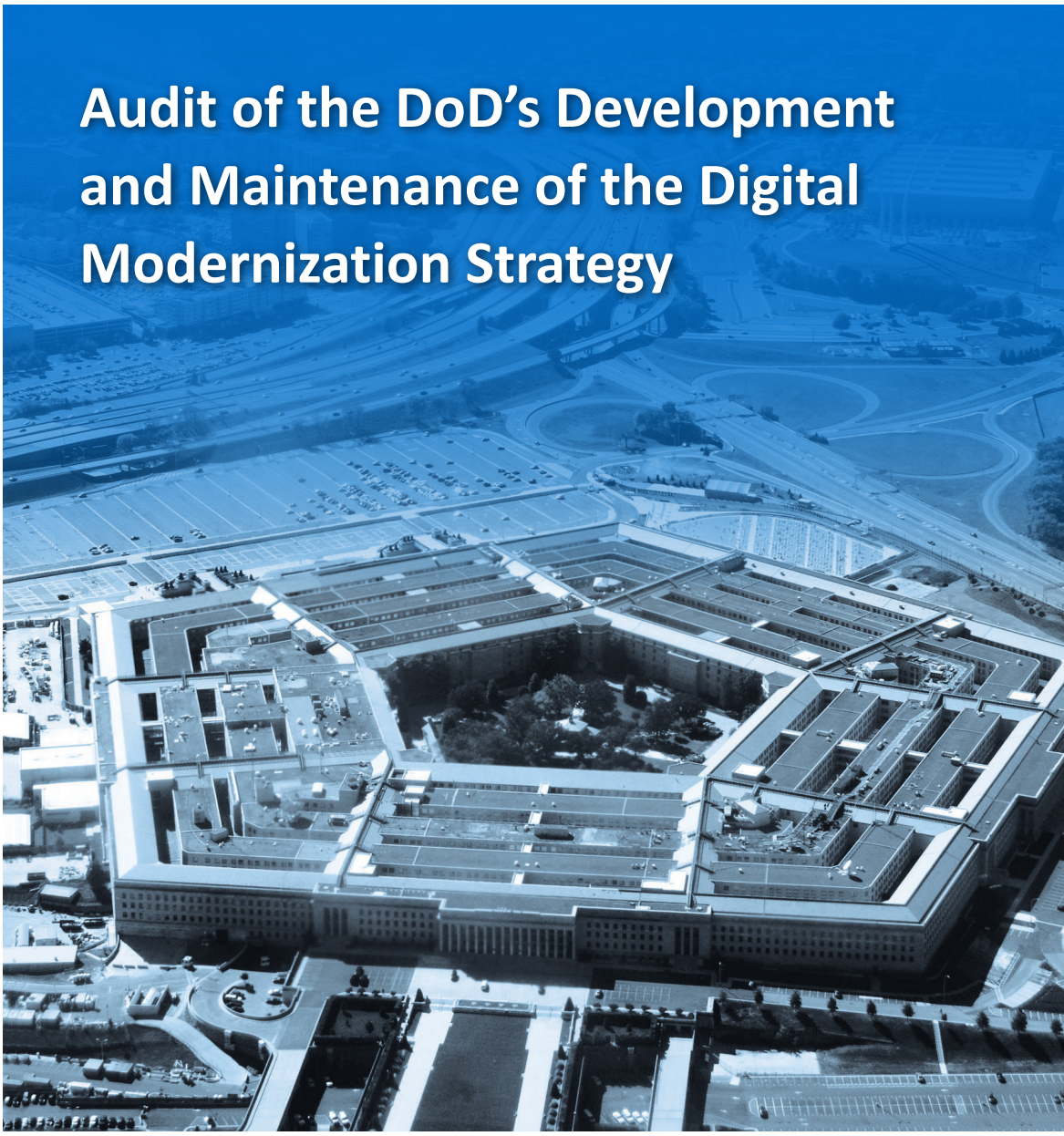
Report No. DODIG-2024-104

INSPECTOR GENERAL

U.S. Department of Defense

JULY 9, 2024

Audit of the DoD's Development and Maintenance of the Digital Modernization Strategy



INDEPENDENCE ★ INTEGRITY ★ EXCELLENCE ★ TRANSPARENCY


INSPECTOR GENERAL
INTEGRITY
EFFICIENCY
DEPARTMENT OF DEFENSE

Results in Brief

Audit of the DoD's Development and Maintenance of the Digital Modernization Strategy

July 9, 2024

Objective

The objective of this audit was to determine whether the DoD developed and maintained the Digital Modernization Strategy (DMS) in accordance with Office of Management and Budget (OMB) Circular No. A-130.

Background

OMB Circular No. A-130, "Managing Information as a Strategic Resource," July 28, 2016, requires each Federal agency to develop and maintain an Information Resource Management (IRM) Strategic Plan to manage its information resources. The Circular requires that the IRM Strategic Plan describe the agency's technology and information resource goals and demonstrate how the goals map to the agency's mission and organizational priorities. The goals must be specific, verifiable, and measurable; and the IRM Strategic Plan must be reviewed annually as part of the agency's Annual Performance Plan review. In July 2019, the Deputy Secretary of Defense, with support from the DoD Chief Information Officer (CIO), issued the DoD's IRM Strategic Plan, known as the DMS, to address those requirements.

Findings

The DoD CIO did not develop or maintain the DMS in accordance with all OMB Circular No. A-130 requirements. Although the DoD CIO ensured that the DMS describes the agency's technology and information resource goals and demonstrates how the goals map to the agency's mission and organizational priorities, the DoD CIO did not:

- ensure that 54 (41 percent) of the 131 strategy elements that support the DMS goals are specific, verifiable, and measurable; or
- conduct annual DMS reviews in FYs 2022 and 2023 or provide support that the reviews were conducted in FYs 2020 and 2021.

Office of the CIO (OCIO) personnel stated that they were unaware that the strategy elements were not specific, verifiable, and measurable and, because of staff turnover, they could not provide support to the DoD OIG that annual DMS reviews were conducted in FY 2020 and FY 2021. According to the former Chief of Staff for the OCIO, DMS reviews were not conducted in FY 2022 and FY 2023 because of changes in OCIO leadership and debate on whether to update the DMS or develop a new one. In addition, the DoD CIO did not designate an official to ensure that the DMS met all OMB Circular No. A-130 requirements.

The DMS should be a centralized and focused path to guide daily decision making to achieve the DoD's digital modernization goals. However, without specific, verifiable, and measurable strategy elements, the DoD cannot meaningfully track progress towards achieving the DMS goals. In addition, by not conducting annual DMS reviews, the DoD may have missed opportunities to update the DMS goals, objectives, or strategy elements based on performance gaps identified during the Annual Performance Plan reviews.

Recommendations

Among other recommendations, we recommended that the DoD CIO develop and implement standard operating procedures that include definitions for specific, verifiable, and measurable. We also recommended that the DoD CIO designate an official from the OCIO to ensure that the DMS meets all OMB Circular No. A-130 requirements.

Results in Brief

Audit of the DoD's Development and Maintenance of the Digital Modernization Strategy

Management Comments and Our Response

The DoD CIO agreed with and provided planned actions to address seven of the recommendations; therefore, the recommendations are resolved but remain open. We will close the recommendations once we verify that management has implemented the agreed-upon actions. The DoD CIO also agreed with and provided information on actions completed to address one recommendation; therefore, the recommendation is closed and no additional action is necessary.

The DoD CIO did not fully address the remaining two recommendations related to defining specific, verifiable, and measurable and establishing requirements for maintaining documentation to support closure of the strategy elements; therefore, they are unresolved. We request that the DoD CIO provide additional comments within 30 days in response to the final report for those two 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, DoD	1.a.i, 1.a.v	1.a.ii, 1.a.iii, 1.a.iv, 1.b, 1.b.i, 1.b.ii, 1.c	1.d

Please provide Management Comments by August 8, 2024.

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** – The DoD OIG verified that the agreed-upon corrective actions were implemented.


INSPECTOR GENERAL
INTEGRITY
EFFICIENCY
DEPARTMENT OF DEFENSE

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

July 9, 2024

MEMORANDUM FOR CHIEF INFORMATION OFFICER, DOD

SUBJECT: Audit of the DoD's Development and Maintenance of the Digital Modernization Strategy (Report No. DODIG-2024-104)

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 report when preparing the final report. These comments are included in the report.

This report contains two recommendations that are considered unresolved because the DoD Chief Information Officer did not fully address the recommendations. We will track these recommendations until management has agreed to take actions that we determine to be sufficient to meet the intent of the recommendations and management officials submit adequate documentation showing that all agreed-upon actions are completed.

DoD Instruction 7650.03 requires that recommendations be resolved promptly. Therefore, within 30 days please provide us your response concerning specific actions in process or alternative corrective actions proposed on the two unresolved recommendations. Send your response to either followup@dodig.mil if unclassified or rfunet@dodig.smil.mil if classified SECRET.

This report contains seven recommendations that we consider resolved and open. We will close these recommendations when the DoD Chief Information Officer provides us documentation showing that all agreed-upon actions are completed. Therefore, within 90 days please provide us your response concerning specific actions completed on the seven resolved recommendations. Send your response to either followup@dodig.mil if unclassified or rfunet@dodig.smil.mil if classified SECRET.

If you have any questions, please contact me at [redacted]. We appreciate the cooperation and assistance received during the audit.

FOR THE INSPECTOR GENERAL:

Carol N. Gorman
Assistant Inspector General for Audit
Cyberspace Operations

Contents

Introduction

Objective

The objective of this audit was to determine whether the DoD developed and maintained its Digital Modernization Strategy (DMS) in accordance with Office of Management and Budget (OMB) Circular No. A-130 requirements. See Appendix A for a discussion of the scope and methodology.

Background

OMB Circular No. A-130 requires each Federal agency to develop and maintain an Information Resource Management (IRM) Strategic Plan to manage and maintain its information resources.[1] The Circular states that the IRM Strategic Plan must describe the agency's technology and information resource goals and demonstrate how the goals map to the agency's mission and organizational priorities. The Circular requires that the goals be specific, verifiable, and measurable so that the agency can track its progress in accomplishing the goals.[2] The Circular also requires each agency to review its IRM Strategic Plan on an annual basis alongside its Annual Performance Plan reviews to determine whether there are any performance gaps or changes to mission needs, priorities, or goals.[3]

The Digital Modernization Strategy

In July 2019, the Deputy Secretary of Defense, with support from the DoD Chief Information Officer (CIO), issued the DoD's IRM Strategic Plan, known as the DMS.[4] The DMS establishes a framework for the DoD designed to achieve a secure, effective, and efficient DoD digital environment with a focus on the following four goals.

- **Innovate for Competitive Advantage** – Implement information technologies that will improve military operations.
- **Optimize for Efficiencies and Improved Capability** – Adopt industry best practices and proven technologies to enhance DoD information technology (IT) operations.

[1] OMB Circular No. A-130, "Managing Information as a Strategic Resource," July 28, 2016.

[2] OMB Circular No. A-130 does not define "specific," "verifiable," or "measurable"; therefore, for the purposes of this report, we used the definitions from the Merriam-Webster dictionary. See the section, "Assessment of the Strategy Elements," of this report for those definitions.

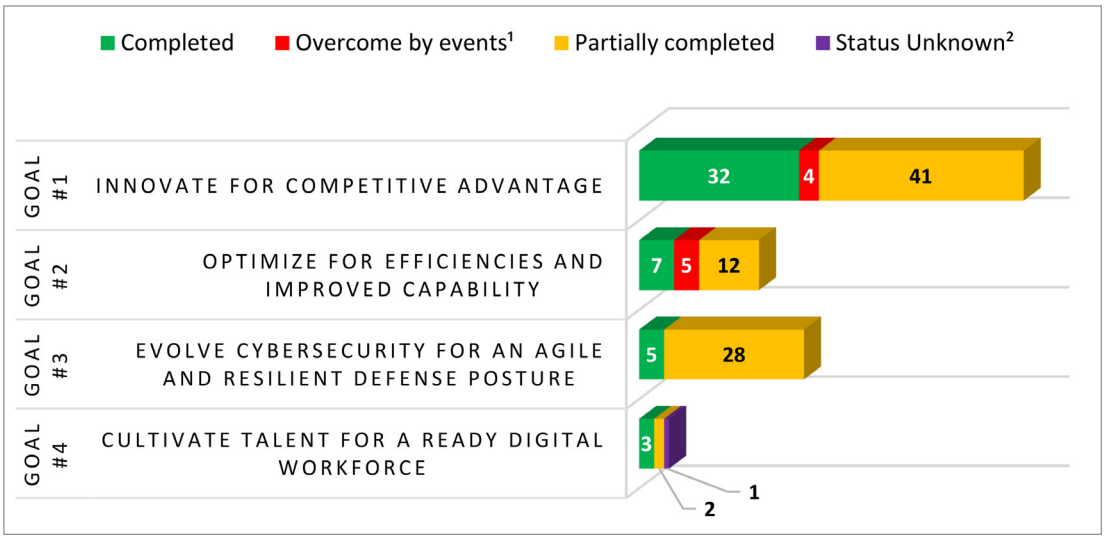
[3] OMB Circular No. A-11, "Preparation, Submission, and Execution of the Budget," August 11, 2023, requires each Federal Agency to prepare an Annual Performance Plan in conjunction with the annual budget submission process. The Annual Performance Plan describes the agency's strategies, performance targets, and key milestones that will be accomplished in the current and following fiscal years.

[4] DoD Digital Modernization Strategy, "DoD Information Resource Management Strategic Plan FY19-23," July 12, 2019.

- **Evolve Cybersecurity for an Agile and Resilient Defense Posture** – Reform DoD cybersecurity policies and processes, modernize its cybersecurity capabilities, and support the DoD and its contractors to defend DoD systems against sophisticated adversaries.
- **Cultivate Talent for a Ready Digital Workforce** – Enhance DoD recruiting, retention, and training processes to provide a well-trained, highly qualified IT workforce.

The DMS goals have 27 corresponding objectives and 140 tasks listed under the objectives known as "strategy elements." The DMS states that each objective provides a rationale for the work the DoD plans to perform and a description of what the objective will accomplish. Additionally, the DMS states that the strategy elements are "specific, focused initiatives needed to accomplish a particular objective." As of December 12, 2023, the Office of the Chief Information Officer (OCIO) reported its progress in completing the strategy elements, which is summarized in Figure 1. Appendix B provides a list of the goals, objectives, strategy elements, and their completion statuses according to the OCIO progress report.

Figure 1. OCIO's Reported Progress in Completing Strategy Elements for DMS Goals



[1] OCIO officials stated that the strategy elements identified as "overcome by events" are those that were merged into other strategy elements or that were reassigned to another DoD Component for action and no longer tracked in the DMS.

[2] The OCIO did not provide a status for strategy element 4.1.2, Identify and Target Work Role Gaps of Critical Need for the Cyber (IT and Cybersecurity) Workforce.

Source: The DoD OIG.

Because the DMS states that the strategy elements are the specific, focused initiatives needed to accomplish the DMS objectives and ultimately the DMS goals, we analyzed whether the 131 strategy elements tracked in the DMS (140 original strategy elements less the 9 considered overcome by events) were specific, verifiable, and measurable when determining compliance with the applicable OMB Circular No. A-130 requirement.

DMS Roles and Responsibilities

According to DoD Directive 5144.02, "DoD Chief Information Officer (DoD CIO)," the DoD CIO is responsible for all matters relating to the DoD information enterprise, which includes developing, implementing, and monitoring the execution of the DMS.[5] According to OCIO personnel, the Director of the DoD Information Network Modernization Directorate was designated the responsibility for developing the DMS.[6] The DoD CIO assigned the following four governance boards the responsibility to track the progress and completion statuses of the DMS strategy elements.

- **Chief Digital and Artificial Intelligence Officer** – Manages the strategy elements to enhance data analytics in support of senior leader decision making and warfighting operations.[7]
- **Command, Control, and Communications Leadership Board** – Manages the strategy elements to modernize command, control, communications, and computer systems; enhances protection for positioning, navigation, and timing capabilities; and enhances mobile device capabilities.
- **Digital Modernization Infrastructure Executive Committee** – Manages the strategy elements to modernize DoD control systems, networks, and other infrastructure in support of DoD cloud, artificial intelligence, command and control, cybersecurity, and data capabilities.
- **Information Security Risk Management Committee** – Manages the strategy elements to reform DoD Risk Management Framework processes, protects unclassified networks, and strengthens the DoD cyber and IT acquisition workforce.

Appendix B identifies the governance board responsible for each of the strategy elements.

[5] DoD Directive 5144.02, "DoD Chief Information Officer," September 19, 2017.

[6] The DoD Information Network Modernization Directorate is an office under the Deputy Chief Information Officer for Information Enterprise.

[7] On February 1, 2022, the Office of the Secretary of Defense established the Office of the Chief Digital and Artificial Intelligence Officer. The Office of the Chief Digital and Artificial Intelligence Officer serves as the successor organization to the Joint Artificial Intelligence Center and Chief Data Officer Council.

Assessment of the Strategy Elements

OMB Circular No. A-130 did not define the terms "specific," "verifiable," and "measurable." Therefore, for the purposes of this report, we used the following definitions from the Merriam-Webster dictionary to determine whether a strategy element was specific, verifiable, and measurable.[8]

- **Specific** – free from ambiguity (unambiguous). Synonyms for unambiguous include clear and precise.
- **Verifiable** – capable of establishing or demonstrating to be true or accurate. Synonyms for verifiable include confirmable and supportable.
- **Measurable** – capable of being measured – able to be described in specific terms (as of size, amount, duration, or mass) usually expressed as a quantity.

[8] Merriam-Webster, Incorporated, "Merriam-Webster.com Dictionary," (No Date Available).

Finding

The DoD CIO Did Not Develop or Maintain the DMS in Accordance with All OMB Circular No. A-130 Requirements

The DoD CIO did not develop or maintain the DMS in accordance with all OMB Circular No. A-130 requirements. Although the DoD CIO ensured that the DMS describes the agency's technology and information resource goals and demonstrates how the goals map to the agency's mission and organizational priorities, the DoD CIO did not:

- ensure that 54 (41 percent) of the 131 strategy elements that support the DMS goals are specific, verifiable, and measurable; or
- conduct annual DMS reviews in FYs 2022 and 2023 or provide support that the reviews were conducted in FYs 2020 and 2021.

OCIO personnel stated that they were unaware that the strategy elements were not specific, verifiable, and measurable and, because of staff turnover, they could not provide support that the annual DMS reviews were conducted in FY 2020 and FY 2021. According to the former Chief of Staff for the OCIO, DMS reviews were not conducted in FY 2022 and FY 2023 because of changes in OCIO leadership and debate at the time on whether to update the DMS or develop a new one.[9] In addition, the DoD CIO did not designate an official to ensure that the DMS met all OMB Circular No. A-130 requirements.

Modernizing its digital environment is crucial for the DoD to ensure the Joint Force has a competitive advantage in the modern battlespace. The DMS should create a centralized and focused path to guide daily decision making to achieve DoD's digital modernization goals. However, without specific, verifiable, and measurable strategy elements, the DoD cannot meaningfully track progress towards achievement of DMS goals. In addition, by not conducting annual DMS reviews in conjunction with the DoD's Annual Performance Plan reviews, the DoD missed opportunities to identify performance gaps or changes to mission needs, priorities, goals, objectives, or strategy elements that required updates to the DMS.

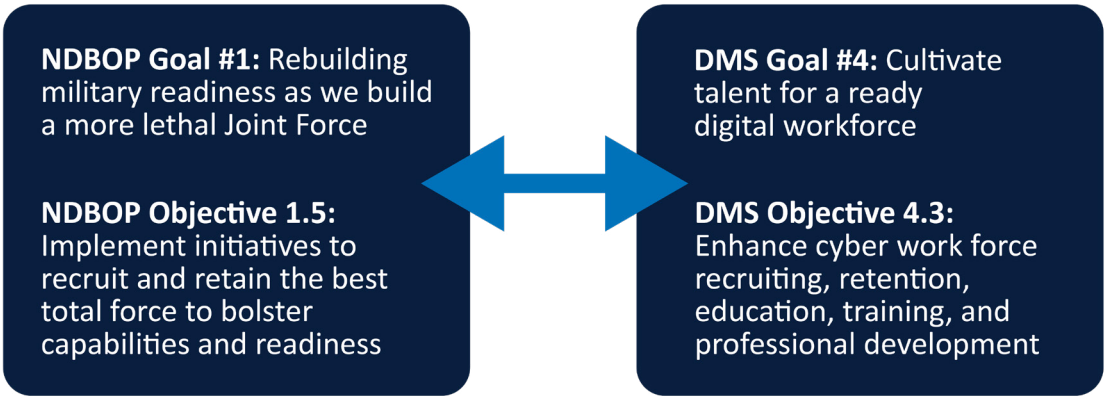
[9] OCIO officials stated that the DoD will publish a new DMS in FY 2024.

The DMS Describes and Maps Resource Goals to DoD Priorities

The DMS describes the DoD's technology and information resource goals and demonstrates how those goals map to the DoD's mission and organizational priorities, as required by OMB Circular No. A-130.[10] The DoD's mission and organizational priorities are established in the National Defense Business Operations Plan (NDBOP) for FYs 2018-2022, which served as the DoD's Agency Strategic Plan for FYs 2018-2022.[11]

To determine whether the DoD CIO complied with the Circular, we reviewed the DMS to ensure that it described the DoD's technology and information resource goals. Next, we compared the DMS to the NDBOP to ensure that the DoD CIO demonstrated how the goals mapped to the DoD's mission and organizational priorities. The DMS contains a description of each goal, its mission impact, and identifies the NDBOP goal to which it relates. The DMS also includes an appendix that maps 3 NDBOP goals and 6 of the 9 objectives to the 4 DMS goals and 27 objectives.[12] Figure 2 provides an example of how the DoD mapped an NDBOP goal and objective to a DMS goal and objective.

Figure 2. Example of an NDBOP Goal and Objective Mapped to a DMS Goal and Objective



Source: The DoD OIG.

[10] OMB Circular No. A-130, Section 5.a.1, "Strategic Planning."

[11] An Agency Strategic Plan is a plan that presents an agency's long-term objectives to accomplish under an Administration. We used the FYs 2018-2022 NDBOP to determine whether the DMS mapped to DoD priorities because that was the strategic plan in place when the DMS was developed. The DoD published the FYs 2022 – 2026 Strategic Management Plan in July 2022; however, OCIO personnel did not update the DMS to align with the new plan.

[12] The three objectives that OCIO personnel did not include in the DMS are "Restore Military Readiness to Build a More Lethal Force," "Reform the Security Cooperation Enterprise," and "Optimize Organizational Structures."

The DMS Strategy Elements Are Not Always Specific, Verifiable, and Measurable

The DoD CIO did not ensure that all of the DMS strategy elements are specific, verifiable, and measurable as required by OMB Circular No. A-130.[13] Specifically, of the 131 strategy elements we analyzed, 77 (59 percent) are specific, verifiable, and measurable and 54 (41 percent) are not.

The DMS Contains 77 Strategy Elements That Are Specific, Verifiable, and Measurable

The DMS contains 77 strategy elements that are specific, verifiable, and measurable. Table 1 includes examples of our analysis of four of those strategic elements.

Table 1. Strategy Element Analysis

Strategy Element	Specific	Verifiable	Measurable
1.1.1—Stand up the Joint Artificial Intelligence Center (JAIC) and Initiate Operations	The strategy element is specific because "Stand up" and "Initiate Operations" are clear and precise terms. In this context, stand up means to establish.	The strategy element is verifiable because the DoD could demonstrate when the JAIC was established and began operations.	The strategy element is measurable because the DoD could determine the amount of progress made towards the JAIC beginning operations.
1.7.2—Develop and Publish the DoD Positioning, Navigation, and Timing Science and Technology Roadmap in Coordination with the Under Secretary of Defense for Research and Engineering	The strategy element is specific because "Develop" and "Publish" are clear and precise terms.	The strategy element is verifiable because the DoD could demonstrate that it published the roadmap.	The strategy element is measurable because the DoD could determine the amount of progress made towards publishing the roadmap.
1.2.4—Establish an Enterprise Cloud Office to Enable Rapid Acquisition, Deployment, and Migration to Cloud Capabilities	The strategy element is specific because "Establish" is a clear and precise term.	The strategy element is verifiable because the DoD could demonstrate that it established an Enterprise Cloud Office with responsibilities to enable cloud capabilities.	The strategy element is measurable because the DoD could determine the amount of progress made towards establishing an Enterprise Cloud Office with responsibilities to enable cloud capabilities.

[13] OMB Circular No. A-130, Section 5.a.1.

Table 1. Strategy Element Analysis (cont'd)

Strategy Element	Specific	Verifiable	Measurable
3.1.6—Standardize on Windows 10 Secure Host Baseline	The strategy element is specific because "Standardize" in this context means to ensure that there is one defined process for installing Windows 10 across the DoD.	The strategy element is verifiable because the DoD could demonstrate that it issued a DoD-wide instruction for installing Windows 10.	The strategy element is measurable because the DoD could determine the amount of progress made towards developing and issuing the DoD-wide instruction.

Source: The DoD OIG.

Because the strategy elements are specific, verifiable, and measurable, the DoD could track the progress in completing the elements and confirm the elements were completed. For example, we reviewed the support for closing two of the strategy elements described above and were able to confirm that the DoD had completed the strategy elements.

- **Strategy element 1.1.1**—OCIO personnel provided us with a copy of the memorandum establishing the JAIC and project documentation that demonstrated the work that the JAIC was performing.
- **Strategy element 1.7.2**—OCIO personnel provided us with a copy of the published roadmap.

The DMS Contains 54 Strategy Elements That Are Not Specific, Verifiable, and Measurable

The DMS contains 54 strategy elements that are not specific, verifiable, and measurable. Table 2 includes examples of our analysis of four of those strategy elements.

Table 2. Strategy Element Analysis

Strategy Element	Specific	Verifiable	Measurable
1.4.2—Invest in and Maintain the Infrastructure Required to Make the DoD's Data Visible, Accessible, Understandable, Trusted, and Interoperable	The strategy element is not specific because "Invest in" and "Maintain" are not clear and precise terms. "Invest in" is not precise without a value or some other quantifiable measure. "Maintain" is an indefinite term in this context.	The strategy element is not verifiable because the DoD cannot support completion of the investment in and maintenance of the required infrastructure without quantifiable measures or a specified end result.	The strategy element is not measurable because the DoD cannot determine the amount of progress made towards completion of the investment in and maintenance of the required infrastructure without quantifiable measures or a specified end result.
1.3.7—Modernize the Global Command and Control System – Joint	The strategy element is not specific because "Modernize" is not a clear or precise term and it is an indefinite term in this context.	The strategy element is not verifiable because the DoD cannot support completion of the modernization efforts without quantifiable measures or a specified end result.	The strategy element is not measurable because the DoD cannot determine the amount of progress made towards modernizing the system without quantifiable measures or a specified end result.
1.13.4—Monitor and Enforce Compliance with Revised Processes, Governance, Policy, and Standards	The strategy element is not specific because "Monitor" and "Enforce" are not clear or precise terms and are indefinite terms in this context.	The strategy element is not verifiable because the DoD cannot support completion of the monitoring or enforcement process without quantifiable measures or a specified end result.	The strategy element is not measurable because the DoD cannot determine the amount of progress made towards the monitoring and enforcing process without quantifiable measures or a specified end result.
3.1.5—Strengthen Data Center Security	The strategy element is not specific because "Strengthen" is not a clear or precise term and is an indefinite term in this context.	The strategy element is not verifiable because the DoD cannot support the level of progress made towards completion of strengthening data center security without quantifiable measures or a specified end result.	The strategy element is not measurable because the DoD cannot determine the amount of progress made strengthening data center security without quantifiable measures or a specified end result.

Source: The DoD OIG.

Although the 54 strategy elements are not specific, verifiable, and measurable, OCIO personnel reported that 17 of the 54 elements are complete, including the 4 strategy elements discussed above. We requested that OCIO provide documentation supporting the closure of two of those strategy elements but, based on the documentation and other support provided, we could not confirm that the DoD had completed the strategy elements.

- **Strategy element 1.4.2, "Invest In and Maintain the Infrastructure Required to Make DoD's Data Visible, Accessible, Understandable, Trusted, and Interoperable."** OCIO personnel provided the 2020 DoD Data Strategy, a memorandum from the Secretary of Defense, and other strategic level documentation to support that the strategy element was completed.[14] Although the documentation explained the DoD's commitment to making DoD data accessible, it was not sufficient to support that the DoD CIO completed the strategy element because the investment amount was not quantified and maintaining infrastructure is a continuous effort.
- **Strategy element 1.13.4, "Monitor and Enforce Compliance with Revised Processes, Governance, Policy, and Standards."** OCIO personnel stated that the DoD developed and implemented various standard operating procedures, instructions, and other documents to demonstrate completion of the strategy element. However, OCIO personnel were unable to provide any of those documents. Even if they had been provided, they would not be sufficient to support that the DoD CIO completed the strategy element because monitoring and enforcing compliance with processes, governance, policy, and standards is a continuous effort.

Therefore, the DoD CIO should develop and implement standard operating procedures that include definitions for "specific," "verifiable," and "measurable." Once the DoD CIO has issued those definitions, they should direct an OCIO official to review the 54 strategy elements that we determined are not specific, verifiable, and measurable, and:

a. revise the 37 strategy elements that are not closed to make them specific, verifiable, and measurable; and

b. determine whether adequate support exists to substantiate the completed status for the 17 remaining strategy elements and, if not, reopen and revise the strategy elements to be specific, verifiable, and measurable.

[14] Department of Defense, "DoD Data Strategy," September 30, 2020. Deputy Secretary of Defense Memorandum, "Creating Data Advantage," May 5, 2021.

The DoD CIO Did Not Conduct DMS Annual Reviews

The DoD CIO did not conduct annual reviews of the DMS in FYs 2022 and 2023 as part of the DoD Annual Performance Plan review, and OCIO personnel could not provide documentation supporting that reviews were conducted in FYs 2020 and 2021. OMB Circular No. A-130 requires that agencies review their IRM Strategic Plan annually alongside the Annual Performance Plan reviews to determine whether there are any performance gaps or changes to mission needs, priorities, or goals.[15] According to the former Chief of Staff for the OCIO, DMS reviews were not conducted in FY 2022 and FY 2023 because of changes in OCIO leadership and debate on whether to update the DMS or develop a new one. Although the DoD Annual Performance Plan reviews for FYs 2020 and 2021 included discussion of the DMS, OCIO personnel could not provide documentation supporting that the DMS was reviewed alongside the Annual Performance Plan or that OCIO personnel identified performance gaps in the DMS based on changes to DoD mission needs, priorities, or goals. Therefore, the DoD CIO should direct an OCIO official to revalidate that the mission needs, priorities, and goals of the DMS map to the current DoD Agency Strategic Plan and update the DMS accordingly.

The DoD CIO Did Not Designate an Official Responsible for Ensuring DMS Compliance with OMB Circular No. A-130

The DoD CIO did not designate an official to ensure that the DMS met all OMB Circular No. A-130 requirements. Although the DoD CIO could not provide a specific date, they plan to publish the FYs 2024-2028 DMS in FY 2024. The DoD CIO could ensure compliance with OMB Circular No. A-130 by designating an official to oversee the development of the updated DMS and issuing standard operating procedures on the annual review process and documentation requirements for closing the strategy elements. Therefore, the DoD CIO should designate an OCIO official to oversee the development and maintenance of the DMS updates. The DoD CIO should also develop and implement standard operating procedures that include, at a minimum:

i. steps for reviewing the DMS annually alongside the DoD's Annual Performance Plan to determine whether there are any performance gaps or changes to mission needs, priorities, or goals;

ii. steps for documenting actions taken to address performance gaps between the DMS and the DoD's Annual Performance Plan;

[15] OMB Circular No. A-130, Section 5.a.1.

iii. steps for documenting their annual reviews, such as including a signature date on the DMS; and

iv. requirements for the Governance Boards to maintain and submit documentation to the OCIO designee to support closure of the strategy elements.

The DMS DoD CIO Cannot Track Progress for Achieving DMS Goals

Modernizing its digital environment is crucial for the DoD to ensure the Joint Force has a competitive advantage in the modern battlespace. The DMS is critical because it should create a centralized and focused path to guide daily decision making to achieve DoD's digital modernization goals. Without specific, verifiable, and measurable strategy elements, the DoD cannot meaningfully track progress towards achievement of DMS goals. In addition, by not conducting annual DMS reviews in conjunction with DoD's Annual Performance Plan reviews, the DoD missed opportunities to identify performance gaps or changes to mission needs, priorities, goals, objectives, or strategy elements that require updates.

Recommendations, Management Comments, and Our Response

Recommendation 1

We recommend that the DoD Chief Information Officer:

a. Develop and implement standard operating procedures that include, at a minimum:

i. Definitions for "specific," "verifiable," and "measurable";

ii. Steps for reviewing the Digital Modernization Strategy annually alongside the DoD's Annual Performance Plan to determine whether there are any performance gaps or changes to mission needs, priorities, or goals;

iii. Steps for documenting actions taken to address performance gaps between the Digital Modernization Strategy and the DoD's Annual Performance Plan;

iv. Steps for documenting their annual reviews, such as including a signature date on the Digital Modernization Strategy; and

v. Requirements for the Governance Boards to maintain and submit documentation to the Office of the Chief Information Officer designee to support closure of the strategy elements.

DoD Chief Information Officer Comments

The DoD CIO agreed, stating that they directed the Deputy Chief Experience Officer (DCXO) to develop and implement standard operating procedures that include performing and documenting annual DMS reviews and addressing performance gaps. The DoD CIO expects to complete these actions by August 30, 2024.

Our Response

Comments from the DoD CIO addressed the specifics of Recommendations 1.a.ii, 1.a.iii, and 1.a.iv; therefore, the recommendations are resolved but open. We will close the recommendations once the DoD CIO provides a copy of the standard operating procedure that includes requirements to conduct annual DMS reviews and address the performance gaps.

Comments from the DoD CIO did not address the specifics of Recommendations 1.a.i, and 1.a.v; therefore, the recommendations are unresolved. The DoD CIO did not specify that the standard operating procedures would include definitions for specific, verifiable, and measurable or include requirements for maintaining documentation to support closure of the strategy elements. Therefore, we request that the DoD CIO provide comments within 30 days of the final report to confirm that the definitions and closure requirements will be included in the standard operating procedures.

b. Direct an official from the Office of the Chief Information Officer to review the 54 strategy elements that we determined are not specific, verifiable, and measurable (once the DoD Chief Information Officer has issued approved definitions for "specific," "verifiable," and "measurable"), and:

i. Revise the 37 strategy elements that are not closed to make them specific, verifiable, and measurable; and

ii. Determine whether adequate support exists to substantiate the completed status for the 17 remaining strategy elements and, if not, reopen and revise the strategy elements to be specific, verifiable, and measurable.

DoD Chief Information Officer Comments

The DoD CIO agreed, stating that they directed the DCXO to facilitate a review of the 54 strategy elements and revise the 37 open strategy elements to meet the approved definitions for specific, verifiable, and measurable. The DoD CIO also stated that the DCXO would provide documentation to substantiate the completed status for the 17 closed strategy elements. The DoD CIO expects to complete these actions by September 27, 2024.

Our Response

Comments from the DoD CIO addressed the specifics of the recommendation; therefore, the recommendation is resolved but open. We will close the recommendation once the CIO provides documentation verifying that the DCXO has completed their review of the 54 strategy elements and made revisions as needed for any strategy element that does not meet the definition of specific, verifiable, or measurable as defined by the DoD CIO in response to Recommendation 1.a.i.

c. Direct an official from the Office of the Chief Information Officer to revalidate that the mission needs, priorities, and goals of the Digital Modernization Strategy map to the current DoD Agency Strategic Plan and update the Digital Modernization Strategy accordingly.

DoD Chief Information Officer Comments

The DoD CIO agreed, stating that they are in the process of finalizing a replacement for the DMS. They stated that the DMS replacement will include four lines of effort which will align with the DoD Strategic Management Plan. The DoD CIO expects to complete this action by July 2024.

Our Response

Comments from the DoD CIO addressed the specifics of the recommendation; therefore, the recommendation is resolved but open.[16] We will close the recommendation once the DoD CIO provides a copy of the DMS replacement, and we verify that it maps to the current DoD Strategic Management Plan.

d. Designate an official from the Office of the Chief Information Officer to oversee the development and maintenance of the Digital Modernization Strategy updates.

DoD Chief Information Officer Comments

The DoD CIO agreed, stating that the DCXO was designated to oversee and administer the development and maintenance of the DMS replacement.

Our Response

Comments from the DoD CIO addressed the specifics of the recommendation. In addition, the DoD CIO provided an action memo, dated May 14, 2024, designating the DCXO to oversee the development and maintenance of the DMS replacement. Therefore, the recommendation is closed.

[16] The DoD Strategic Management Plan is the name of the current version of the DoD Agency Strategic Plan.

Appendix A

Scope and Methodology

We conducted this performance audit from May 2023 through March 2024 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 objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective.

To achieve our audit objective, we reviewed OMB Circular No. A-130 to gain an understanding of the DoD CIO's requirement for developing and maintaining the IRM, including:

- writing specific, verifiable, and measurable goals; and
- reviewing the IRM Strategic Plan annually.

We reviewed the DoD's IRM Strategic Plan, known as the DMS, to determine whether the DoD CIO described the DoD's technology and information resource goals and mapped the goals to the DoD's mission and organizational priorities in the DMS. We also compared the DMS to the FYs 2018-2022 NDBOP because the NDBOP contained the DoD's mission and organizational priorities and served as the DoD's Agency Strategic Plan for FYs 2018 to 2022. We interviewed DoD OCIO personnel, including the former Chief of Staff, to gain an understanding of how the DoD CIO developed and maintained the DMS between FYs 2019 and 2023. We also interviewed OCIO personnel to determine whether they conducted annual DMS reviews.

We requested that OCIO personnel to provide us with a status of each of the 140 DMS strategy elements, which we summarized in Figure 1 of the report. We analyzed 131 of the strategy elements to determine whether they were specific, verifiable, and measurable. We did not analyze the other nine elements because OCIO officials stated that those strategy elements were merged into other elements or reassigned to another DoD Component for action and no longer tracked in the DMS. Since OMB Circular No. A-130 did not define the terms "specific," "verifiable," and "measurable," we used the Merriam-Webster dictionary to define the terms and used those definitions to evaluate compliance with the Circular.

We selected a nonstatistical sample of four strategy elements that OCIO personnel identified as complete. We requested that OCIO personnel provide documentation that adequately demonstrated the strategy element tasks were completed

and appropriately considered closed as reported. In addition, we requested documentation to support whether the DoD CIO reviewed the DMS annually alongside the Annual Performance Plan to determine whether there were performance gaps or changes to mission needs, priorities, or goals.

Internal Control Assessment and Compliance

We assessed internal controls and compliance with laws and regulations necessary to satisfy the audit objective. We identified deficiencies in the underlying principles of implementing control activities and performing monitoring activities. Specifically, we identified several internal control deficiencies related to the process for developing and maintaining the DMS. However, because our review was limited to these internal control components and underlying principles, it may not have disclosed all internal control deficiencies that may have existed at the time of this audit.

Use of Computer-Processed Data

We did not use computer-processed data to perform this audit.

Prior Coverage

During the last 5 years, the Director, Operational Test & Evaluation (DOT&E) issued three reports related to our audit objective. Unrestricted DOT&E reports can be accessed at https://www.dote.osd.mil/. The audit team identified the following findings and recommendations that relate to the objectives of the audit of the DoD's development and maintenance of the DMS.

DOT&E

FY 2022 Annual Report, January 2023

> The DOT&E issued its FY 2022 Annual Report summarizing operational test and evaluation activities of the DoD during the preceding fiscal year. The Director identified that many DMS efforts lacked an overarching systems integration process, test strategy, and program executive organization to manage cost, drive schedules, and monitor performance factors. The Director recommended that the DoD CIO and other DoD stakeholders manage DMS initiatives with trained program managers and supporting offices.

FY2021 Annual Report, January 2022

> The DOT&E issued its FY 2021 Annual Report summarizing operational test and evaluation activities of the DoD during the preceding fiscal year. The Director identified that many DMS efforts lacked an overarching systems integration process, test strategy, and program executive organization to manage cost, drive

schedules, and monitor performance factors. The Director recommended that the DoD CIO and other DoD stakeholders manage DMS initiatives with trained program managers and supporting offices.

FY 2020 Annual Report, January 2021

The DOT&E issued its FY 2021 Annual Report summarizing operational test and evaluation activities of the DoD during the preceding fiscal year. The Director identified that many DMS efforts lacked an overarching systems integration process, test strategy, and program executive organization to manage cost, drive schedules, and monitor performance factors. The Director recommended that the DoD CIO and other DoD stakeholders manage DMS initiatives.

Appendix B

DMS Goals, Objectives, and Strategy Element Statuses

The following tables show the DMS goals, objectives, strategy elements, and related completion statuses. The audit team obtained the status of each strategy element from OCIO personnel and organized the following four tables by assigned governance board (green square ■=complete, orange triangle ▲=partially completed, red circle ●=overcome by events, purple diamond ◆=status unknown).

Table 3. Goals, Objectives, and Status of Strategy Elements Managed by the Chief Digital and Artificial Intelligence Office

Goal	Objective	Strategy Element	Status Color
Innovate for Competitive Advantage	Establish the JAIC to Accelerate Adoption and Integration of AI-Enabled Capabilities to Achieve Mission Impact at Scale	1.1.1. Stand Up the JAIC and Initiate Operations	■
		1.1.2. Establish Partnerships with Industry, Academia, and Partner Nations to Ensure State-of-the-Art AI Capabilities	■
		1.1.3. Develop and Sustain the Enterprise Infrastructure Technology Stack that Enables AI Capability Deployment at Speed and Scale (JAIC Common Foundation)	■
		1.1.4. Lead DoD in AI Planning, Policy, Oversight, Ethics, and Safety	▲
		1.1.5. Deliver AI-Enabled Capabilities to Address Key Missions (National Mission Initiatives, Component Mission Initiatives, and Smart Automation Initiatives)	▲
		1.1.6. Assure / Certify the AI Algorithms, Data, and Models Developed for JAIC Implementations	■
Innovate for Competitive Advantage	Treat Data as a Strategic Asset	1.4.1. Define a Minimum Essential Set of Enterprise Data Tags that Enable the Tenets of Department of Defense Instruction 8320.07	■
		1.4.2. Invest In and Maintain the Infrastructure Required to Make DoD's Data Visible, Accessible, Understandable, Trusted, and Interoperable	■

LEGEND

AI Artificial Intelligence

Source: The DoD OIG.

Table 4. Goals, Objectives, and Status of Strategy Elements Managed by the Command, Control, and Communications Leadership Board

Goal	Objective	Strategy Element	Status Color
Innovate for Competitive Advantage	Modernize Warfighter C4 Infrastructure and Systems	1.3.1. Produce C4 Strategies, Roadmaps, Plans, and Architectures	▲
		1.3.2. Update and Publish Required Tactical Communications Policies	▲
		1.3.3. Synchronize Enterprise C4 Capabilities through Effective Governance	▲
		1.3.4. Modernize Tactical Radios and DoD Tactical Waveform Capabilities	▲
		1.3.5. Develop and Maintain the Enterprise Architecture for DoD Public Safety Communications	▲
		1.3.6. Implement DoD Global Enterprise Mass Warning & Notification Capabilities	■
		1.3.7. Modernize the Global Command and Control System – Joint	■
		1.3.8. Modernize DoD SATCOM Management and Control	▲
		1.3.9. Execute the SATCOM Modernization Activities Driven by the Protected Satellite Communications Service AoA, the Wideband Communications Services AoA, and the Impending Narrowband Satellite Communications AoA	▲
		1.3.10. Formalize and Implement the Enterprise SATCOM Management and Control Reference Architecture	▲
	Strengthen Collaboration, International Partnerships, & Allied Interoperability	1.5.1. Develop Military Satellite Communications Services, Infrastructure, and Standards with International Partners	▲
		1.5.2. Improve Tactical Communications Waveform Export Processes and Develop a Standardized Method to Address Combatant Command Connection Requests between U.S. and Allied/Coalition Systems	▲
		1.5.5. Develop Flexible and Robust Secure Cryptographic Products for Seamless Secure Foreign Partner Interoperability	▲
		1.5.8. Rationalize Coalition Command and Control and Intelligence Information Sharing Capabilities	▲

Table 4. Goals, Objectives, and Status of Strategy Elements Managed by the Command, Control, and Communications Leadership Board (cont'd)

Goal	Objective	Strategy Element	Status Color
Innovate for Competitive Advantage	Ensure National Leadership Command Capabilities Assured Connectivity	1.6.1. Evaluate Current Conferencing Capability and, If Required, Develop a Methodology that Improves Secure, Survivable Conferencing	▲
		1.6.2. Enhance Current Data Collection and Display Processes to Provide Senior Leadership Quality Decision-Making Information	●
		1.6.3. Develop a Process that Delivers a Classified, Secure, and Mobile Solution that Meets Senior Leadership Requirements	■
		1.6.4. Enhance the Security of the Supply Chain for Continuity of Operations, Continuity of Government, and Senior Leader Command, Control, and Communications System Communications Programs	▲
	Enhance the Delivery and Protection of PNT	1.7.1. Pursue DoD Implementation of a Modular Open Systems Approaches and Collaborative Modeling & Simulation Approach for PNT Capabilities	▲
		1.7.2. Develop and Publish the DoD PNT Science & Technology Roadmap in Coordination with the Under Secretary of Defense for Research & Engineering	■
		1.7.3. Track and Assist in Modifying Plans for Military Global Positioning System User Equipment Development and Production	■
		1.7.4. Field Modernized PNT Capabilities with the Air Force and Our International Allies	▲
		1.7.5. Develop Navigation Warfare Partnerships with Closely Allied Nations	■
		1.7.6. Evaluate and Demonstrate Complementary PNT Capabilities to Support Domestic Critical Infrastructure in Cooperation with Civilian Agencies (Department of Transportation and Department of Homeland Security)	▲
		1.7.7. Exercise the DoD PNT Enterprise Oversight Council, Executive Management Board, and Supporting Working Groups, To Ensure the DoD PNT Enterprise Provides a Military PNT Advantage to the Warfighter	■
		1.7.8. Develop New (and Maintain Existing) DoD Issuances to Facilitate Policy Implementation and Ensure DoD Component Compliance for the DoD PNT Enterprise	■
		1.7.9. Continue to Institutionalize the PNT Data Repository Data Collection Process	■

Table 4. Goals, Objectives, and Status of Strategy Elements Managed by the Command, Control, and Communications Leadership Board (cont'd)

Goal	Objective	Strategy Element	Status Color
Innovate for Competitive Advantage	Improve Information Sharing to Mobile Users	1.11.1. Streamline the Purchasing of Mobile Devices and Services across the DoD Enterprise	▲
		1.11.2. Improve Mobile Policies, Processes, and Procedures to Ensure Efficient and Effective Portfolio Management	▲
		1.11.3. Expand Use of Derived Credentials for Mobile	▲
		1.11.4. Develop Applications of Tactical Mobility	▲
		1.11.5. Establish a Mobile Device Security Architecture and Risk Management Approach in Collaboration with Five Eyes Mission Partners	▲
		1.11.6. Establish DoD Way-Ahead, Policy, and Plans for Use of the National First Responder Network in Support of DoD Public Safety Communications	▲
		1.11.7. DoD Will Be an Early Adopter of 5G and Develop Applications to Leverage 5G Advanced Capabilities	▲
Innovate for Competitive Advantage	Evolve the DoD to Agile EMSO	1.12.1. Establish an EMSO Multi-Tiered Architecture Capable of Sharing EMS Data Between All Services and Agencies at All Classification Levels	▲
		1.12.2. Establish a Resilient, Secure, and Adaptive EMSO IT Network Infrastructure	▲

LEGEND

AoA Analysis of Alternatives
C4 Command, Control, Communications, and Computer
EMSO Electromagnetic Spectrum Operations
PNT Position, Navigation, and Timing
SATCOM Satellite Communications

Source: The DoD OIG.

Table 5. Goals, Objectives, and Status of Strategy Elements Managed by the Digital Modernization Infrastructure Executive Committee

Goal	Objective	Strategy Element	Status Color
Innovate for Competitive Advantage	Deliver a DoD Enterprise Cloud Environment to Leverage Commercial Innovation	1.2.1. Deliver a General-Purpose Enterprise Cloud for Compute and Store Capabilities (i.e., Joint Enterprise Defense Infrastructure)	■
		1.2.2. Identify Common Niche Capabilities to Inform the Creation of Fit for Purpose Cloud Environments	▲
		1.2.3. Provide a DoD On Premise Cloud Environment	■
		1.2.4. Establish an Enterprise Cloud Office to Enable Rapid Acquisition, Deployment, and Migration to Cloud Capabilities	■
		1.2.5. Manage the DoD Portfolio of Cloud Capabilities	▲
		1.2.6. Develop Policy and Guidance to Modernize Application Development (e.g., Lean-Agile Practices)	■
		1.2.7. Develop and Deploy a Development, Security, and Operations Environment that Enables Application Development and Accreditation at Speed and Scale Integrated with Defensive Cyberspace Operations	▲
		1.2.8. Develop Policy and Guidance on the Effective Application of Development, Security, and Operations Principles	■
		1.2.9. Enable Resilient Operation of DoD Functions on Commercial Cloud Infrastructure	■
Innovate for Competitive Advantage	Strengthen Collaboration, International Partnerships, & Allied Interoperability	1.5.3. Advance Civil Emergency Communications Planning with DoD, North Atlantic Treaty Organization, Allies, and Other International Partners	●
		1.5.4. Ensure End-to-End ICAM Interoperability with Key Interagency and International Partners at Appropriate Assurance Levels for the Information Being Shared	▲
		1.5.6. Streamline Release Processes and Decision Making to Advance U.S. Security Cooperation	▲
		1.5.7. Implement the Mission Partner Environment Requirements and Portfolio Management Processes	■
		1.5.9. Deliver the DoD Mission Partner Environment Capability and Services	▲

Table 5. Goals, Objectives, and Status of Strategy Elements Managed by the Digital Modernization Infrastructure Executive Committee (cont'd)

Goal	Objective	Strategy Element	Status Color
Innovate for Competitive Advantage	Modernize DISN Transport Infrastructure	1.8.1. Upgrade Optical Transport	■
		1.8.2. Enhance Mid-Point Security by Implementing Joint Regional Security Stack and Joint Management System	■
		1.8.3. Build Out Multi-Protocol Label Switching Router Network with Quality of Service and Performance Monitoring	■
		1.8.4. Implement Software Defined Networking	▲
		1.8.5. Eliminate Asynchronous Transfer Mode and Low Speed Time Division Multiplexed Circuits	▲
		1.8.6. Implement Internet Protocol Version 6	▲
Innovate for Competitive Advantage	Modernize and Optimize DoD Component Networks and Services	1.9.1. Consolidate and Optimize Fourth Estate Networks	▲
		1.9.2. Consolidate the Number of Fourth Estate Service Desks into a Single Service Support Environment	▲
		1.9.3. Consolidate and Optimize the Fourth Estate Network Operation Centers/ Security Operations Centers	●
		1.9.4. Establish Best Practices for Component Use of Commercial Service Providers in Their Optimization and Modernization Efforts	●
Innovate for Competitive Advantage	Provide End-to-End AISR Data Transport	1.10.1 Establish Capabilities to Support Ingest, Accumulation, and Global Delivery of AISR Data from Multiple Platforms/Sources	■
		1.10.2 Build Tactical Relays for Sensor Platform Connectivity to Local Users and the DISN	▲
		1.10.3 Provide Global Satellite Gateways for Direct Beyond Line of Sight Connectivity Between AISR Platforms and the DISN	■
		1.10.4 Establish Network Operations to Support End-to-End Situational Awareness and Proactive Network Management	▲
		1.10.5. Provide Direction for Future Platform Transport Capabilities	■

Table 5. Goals, Objectives, and Status of Strategy Elements Managed by the Digital Modernization Infrastructure Executive Committee (cont'd)

Goal	Objective	Strategy Element	Status Color
Innovate for Competitive Advantage	Drive Standards into DoD IT Systems	1.13.1. Assess and Identify Gaps in Policy for IT, Networking, Data, and Cybersecurity Standards	■
		1.13.2. Develop Strategy for Addressing Gaps in Processes, Governance, Policy, and Standards	■
		1.13.3. Implement Revised Processes, Governance, Policy, and Standards	■
		1.13.4. Monitor and Enforce Compliance with Revised Processes, Governance, Policy, and Standards	■
Optimize for Efficiencies and Improved Capability	Shift from Component-Centric to Enterprise-Wide Operations and Defense Model	2.1.1. Enable Global and Regional Operations Centers	●
		2.1.2. Establish and Implement the Joint Information Environment Management Network for Joint Regional Security Stack	■
		2.1.3. Converge DoD Information Network Information Technology Service Management Solutions	●
		2.1.4. Converge DoD Information Network Operation Common Operation Picture Solutions	●
Optimize for Efficiencies and Improved Capability	Optimize DoD Data Centers	2.2.1. Migrate DoD Applications and Systems that Cannot be Hosted in Commercial Cloud Environments to Enterprise Data Centers	▲
		2.2.2. Optimize Select Data Centers for Performance First, Then Cost	■
		2.2.3. Re-designate Installation Processing Nodes in Accordance with the Department's Current Data Center Optimization Approach	■
		2.2.4. Manage the DoD Data Center Inventory for Mission Need	■
Optimize for Efficiencies and Improved Capability	Optimize DoD Office Productivity and Collaboration Capabilities (ECAPS Capability Set 1)	2.3.1. Designate Defense Enterprise Office Solution as a DoD Enterprise Service with all DoD Components Required to Adopt	■
		2.3.2. Monitor and Assess All Pilots for Implementation Pitfalls and Challenges, including Denied, Degraded, Intermittent or Limited Bandwidth; Roll All Lessons Learned from Early Cloud Adopters into Defense Enterprise Office Solution	▲
		2.3.3. Field Defense Enterprise Office Solution (including in Denied, Degraded, Intermittent or Limited Bandwidth Environments) and Complete Migration of All DoD Users	▲

Table 5. Goals, Objectives, and Status of Strategy Elements Managed by the Digital Modernization Infrastructure Executive Committee (cont'd)

Goal	Objective	Strategy Element	Status Color
Optimize for Efficiencies and Improved Capability	Optimize DoD Voice and Video Capabilities (ECAPS Capability Sets 2 & 3)	2.4.1. Define and Deploy an Optimized Enterprise Voice and Video Solution across the Department (e.g., ECAPS Capability Sets 2 and 3)	▲
		2.4.2. Define and Deploy an Optimized DoD Command and Control Voice Solution	▲
		2.4.3. Eliminate DoD's Legacy Analog Phone Switch Infrastructure	▲
		2.4.4. Establish DoD Way-Ahead, Policy, and Plans for Employment of Next Generation 9-1-1	▲
Optimize for Efficiencies and Improved Capability	Improve IT Category Management	2.5.1. Continue to Establish Enterprise License Agreements for IT Software, Hardware, Services, and Telecommunications	▲
		2.5.2. Expand Enterprise License Agreements to Address Other IT Categories (e.g., IT Security) Based on OMB Guidance	▲
		2.5.3. Establish DoD Category Management Policy	■
		2.5.4. Implement DoD IT Asset Management	▲
Optimize for Efficiencies and Improved Capability	Improve Rapid Technology Deployment Processes	2.6.1. Streamline the Technology Approval Process	●
		2.6.2. Leverage the Power and Agility of Other Transactional Agreements	●
Optimize for Efficiencies and Improved Capability	Strengthen IT Financial Management Decision Making & Accountability	2.7.1. Support Audit Readiness for Financial and Mixed Systems that Impact Financial Reporting	▲
		2.7.2. Improve Accountability and Auditability for Internal Use Software Investments	▲
		2.7.3. Implement FY2018 National Defense Authorization Act Requirements Regarding Oversight and Certification of Component IT Budgets	■

Table 5. Goals, Objectives, and Status of Strategy Elements Managed by the Digital Modernization Infrastructure Executive Committee (cont'd)

Goal	Objective	Strategy Element	Status Color
Evolve Cybersecurity for an Agile and Resilient Defense Posture	Deploy an End-to-End ICAM Infrastructure	3.2.1. Expand Public Key Enablement Capabilities to Support ICAM	▲
		3.2.10. Enhance the Governance Structure Promoting the Development and Adoption of Enterprise ICAM Solutions	▲
		3.2.11. Create DoD Policies and Standards Clearly Defining Requirements for Identification, Credentialing, Authentication, and Authorization Lifecycle Management	▲
		3.2.2. Implement Automated Account Provisioning	▲
		3.2.3. Implement Support for Approved Multi-Factor Authentication Capabilities	▲
		3.2.4. Enhance Enterprise Identity Attribute Service	■
		3.2.5. Expand the Use of Derived Credentials	■
		3.2.6. Implement a Data Centric Approach to Collect, Verify, Maintain, and Share Identity and Other Attributes	▲
		3.2.7. Improve and Enable Authentication to DoD Networks and Resources through Common Standards, Shared Services, and Federation	▲
		3.2.8. Deploy Shared Services Promoting the Implementation of Enterprise ICAM	▲
		3.2.9. Enable Consistent Monitoring and Logging to Support Identity Analytics for Detecting Insider Threats and External Attacks	▲

LEGEND

AISR Airborne Intelligence, Surveillance, and Reconnaissance
DISN Defense Information Systems Network
ECAPS Enterprise Collaboration and Productivity Services
ICAM Identity, Credential, and Access Management

Source: The DoD OIG.

Table 6. Goals, Objectives, and Status of Strategy Elements Managed by the Information Security Risk Management Committee

Goal	Objective	Strategy Element	Status Color
Evolve Cybersecurity for an Agile and Resilient Defense Posture	Transform the DoD Cybersecurity Architecture to Increase Agility and Strengthen Resilience	3.1.1. Improve Endpoint Security and Continuous Monitoring	▲
		3.1.2. Enhance Enterprise Perimeter Protection Capabilities	▲
		3.1.3. Establish Enterprise Comply-to-Connect Capability	▲
		3.1.4. Deploy Insider Threat Detection Capabilities	▲
		3.1.5. Strengthen Data Center Security	■
		3.1.6. Standardize on Windows 10 Secure Host Baseline	■
		3.1.7. Implement Automated Patch Management	▲
		3.1.8. Enhance Cybersecurity Situational Awareness through Big Data Analytics	▲
		3.1.9. Modernize the Cryptographic Inventory and Supporting Infrastructure	▲
		3.1.10. Incorporate Cloud-Native Capabilities into Defensive Cyberspace Operations	▲
Evolve Cybersecurity for an Agile and Resilient Defense Posture	Protect Sensitive DoD Information & Critical Programs & Technologies on DIB Unclassified Networks and Information Systems	3.3.1. Support Development of Consistent Procedures to Assess Contractor Compliance with Cybersecurity Requirements	▲
		3.3.2. Support Efforts to Update National Institute of Standards and Technology Special Publication 800-171 to Address Advanced Persistent Threats	▲
		3.3.3. Increase Participation in the DIB Cybersecurity Program	▲
		3.3.4. Expand Cybersecurity Threat Information Sharing to Non-Cleared Defense Contractors	▲
		3.3.5. Plan and Execute DIB Cybersecurity Pathfinders	▲

Table 6. Goals, Objectives, and Status of Strategy Elements Managed by the Information Security Risk Management Committee (cont'd)

Goal	Objective	Strategy Element	Status Color
Evolve Cybersecurity for an Agile and Resilient Defense Posture	Reform DoD Cybersecurity Risk Management Policies and Practices	3.4.1. Advance Risk Management Framework Reform to Ensure it is More Efficient and Adaptable	▲
		3.4.2. Ensure Cybersecurity Risks are Planned for and Managed Throughout the Acquisition Lifecycle	▲
		3.4.3. Enhance Processes to Address Enterprise-Wide Supply Chain Risks	▲
		3.4.4. Strengthen the DoD Cybersecurity Portfolio Management Process	■
		3.4.5. Expand the Use of Proven Software and Hardware Assurance Methods	▲
		3.4.6. Build and Maintain Robust International Cybersecurity Cooperation Efforts	▲
		3.4.7. Increase DoD Participation in Setting Federal Government and International Commercial Cybersecurity Standards	▲
Cultivate Talent for a Ready Digital Workforce	Strengthen Cyber Functional Community Management	4.1.1. Implement the Functional Community Maturity Model for the IT and Cybersecurity Categories of the Cyber Workforce	▲
		4.1.2. Identify and Target Work Role Gaps of Critical Need for the Cyber (IT and Cybersecurity) Workforce	◆
Cultivate Talent for a Ready Digital Workforce	Strengthen the IT Acquisition Workforce	4.2.1. Strengthen IT Acquisition Workforce Competencies	■
		4.2.2. Update Curriculum Requirements and Maintain Continuous Learning Capabilities	■
Cultivate Talent for a Ready Digital Workforce	Enhance Cyber Workforce Recruiting, Retention, Education, Training, and Professional Development	4.3.1. Expand Implementation of Cyber Excepted Service	▲
		4.3.2. Implement Cyber Workforce Qualifications Program	■

LEGEND

DIB Defense Industrial Base

Source: The DoD OIG.

Appendix C

Mapping of DMS Goals and Objectives to NDBOP Goals and Objectives

The Table identifies the alignment between the goals and objectives in the FY 2019 DMS and the FYs 2018-2022 NDBOP as presented in Appendix B, Table 2, of the DMS.

FYs 2018-2022 NDBOP Goals	NDBOP Objective	FY 2019 DMS Goals	DMS Objectives
#1: Rebuilding Military Readiness as We Build a More Lethal Joint Force	1.2 Lay the foundation for future readiness through recapitalization, innovation, and modernization	Innovate for Competitive Advantage	Establish the JAIC to Accelerate Adoption and Integration Delivery of AI-Enabled Capabilities to Achieve Mission Impact at Scale
			Deliver a DoD Enterprise Cloud Environment to Leverage Commercial Innovation
			Modernize Warfighter Command, Control, Communications, and Computer Infrastructure and Systems
			Treat Data as a Strategic Asset
			Strengthen Collaboration, International Partnerships, & Allied Interoperability
			Ensure National Leadership Command Capabilities Assured Connectivity
			Enhance the Delivery and Protection of Position, Navigation, and Timing
			Modernize DISN Transport Infrastructure
			Modernize and Optimize DoD Component Networks and Services
			Provide End-to-End AISR DT
			Improve Information Sharing to Mobile Users
			Evolve the DoD to Agile Electromagnetic Spectrum Operations
			Drive Standards into DoD IT Systems
		Optimize for Efficiencies and Improved Capability	Shift from Component-Centric to Enterprise-Wide Operations and Defense Model
			Optimize DoD Data Centers
			Optimize DoD Office Productivity and Collaboration Capabilities (ECAPS Capability Set 1)
			Optimize DoD Voice & Video Capabilities (ECAPS Capability Sets 2 & 3)
			Improve Rapid Technology Deployment Processes

Mapping of DMS Goals and Objectives to NDBOP Goals and Objectives Management Committee (cont'd)

FYs 2018-2022 NDBOP Goals	NDBOP Objective	FY 2019 DMS Goals	DMS Objectives
#1: Rebuilding Military Readiness as We Build a More Lethal Joint Force (cont'd)	1.2 Lay the foundation for future readiness through recapitalization, innovation, and modernization (cont'd)	Evolve Cybersecurity for an Agile and Resilient Defense Posture	Transform the DoD Cybersecurity Architecture to Increase Agility and Strengthen Resilience
			Deploy an End-to-End ICAM Infrastructure
#1: Rebuilding Military Readiness as We Build a More Lethal Joint Force	1.3 Enhance IT and cybersecurity capabilities	Innovate for Competitive Advantage	Establish the JAIC to Accelerate Adoption and Integration Delivery of AI-Enabled Capabilities to Achieve Mission Impact at Scale
			Deliver a DoD Enterprise Cloud Environment to Leverage Commercial Innovation
			Treat Data as a Strategic Asset
			Strengthen Collaboration, International Partnerships, & Allied Interoperability
			Ensure National Leadership Command Capabilities Assured Connectivity
			Enhance the Delivery and Protection of Position, Navigation, and Timing
			Modernize DISN Transport Infrastructure
			Modernize and Optimize DoD Component Networks and Services
			Provide End-to-End AISR DT
			Improve Information Sharing to Mobile Users
		Optimize for Efficiencies and Improved Capability	Shift from Component-Centric to Enterprise-Wide Operations and Defense Model
			Optimize DoD Data Centers
			Optimize DoD Office Productivity and Collaboration Capabilities (ECAPS Capability Set 1)
			Optimize DoD Voice & Video Capabilities (ECAPS Capability Sets 2 & 3)
			Improve Rapid Technology Deployment Processes
		Evolve Cybersecurity for an Agile and Resilient Defense Posture	Transform the DoD Cybersecurity Architecture to Increase Agility and Strengthen Resilience
			Deploy an End-to-End ICAM Infrastructure
			Protect Sensitive DoD Information and Critical Programs and Technologies on DIB Unclassified Networks and Information Systems
			Reform DoD Cybersecurity Risk Management Policies and Practices

Mapping of DMS Goals and Objectives to NDBOP Goals and Objectives Management Committee (cont'd)

FYs 2018-2022 NDBOP Goals	NDBOP Objective	FY 2019 DMS Goals	DMS Objectives
#1: Rebuilding Military Readiness as We Build a More Lethal Joint Force	1.4 Ensure the best intelligence, counterintelligence, and security support to DoD operations	Innovate for Competitive Advantage	Establish the JAIC to Accelerate Adoption and Integration Delivery of AI-Enabled Capabilities to Achieve Mission Impact at Scale
			Modernize Warfighter Command, Control, Communications, and Computer Infrastructure and Systems
			Treat Data as a Strategic Asset
			Modernize DISN Transport Infrastructure
			Modernize and Optimize DoD Component Networks and Services
			Provide End-to-End AISR DT
			Improve Information Sharing to Mobile Users
			Evolve the DoD to Agile Electromagnetic Spectrum Operations
			Drive Standards into DoD IT Systems
		Optimize for Efficiencies and Improved Capability	Shift from Component-Centric to Enterprise-Wide Operations and Defense Model
			Improve Rapid Technology Deployment Processes
		Evolve Cybersecurity for an Agile and Resilient Defense Posture	Transform the DoD Cybersecurity Architecture to Increase Agility and Strengthen Resilience
			Deploy an End-to-End ICAM Infrastructure
			Protect Sensitive DoD Information and Critical Programs and Technologies on DIB Unclassified Networks and Information Systems
			Reform DoD Cybersecurity Risk Management Policies and Practices
#1: Rebuilding Military Readiness as We Build a More Lethal Joint Force	1.5 Implement initiatives to recruit and retain the best total force to bolster capabilities and readiness	Cultivate Talent for a Ready Digital Workforce	Strengthen the Cyber Functional Community Workforce
			Strengthen the IT Acquisition Workforce
			Enhance Cyber Workforce Recruiting, Retention, Education, Training, and Professional Development

Mapping of DMS Goals and Objectives to NDBOP Goals and Objectives Management Committee (cont'd)

FYs 2018-2022 NDBOP Goals	NDBOP Objective	FY 2019 DMS Goals	DMS Objectives
#2: Strengthen Our Alliances & Attract New Partners		Innovate for Competitive Advantage	Strengthen Collaboration, International Partnerships, & Allied Interoperability
		Optimize for Efficiencies and Improved Capability	Improve Rapid Technology Deployment Processes
		Evolve Cybersecurity for an Agile and Resilient Defense Posture	Protect Sensitive DoD Information and Critical Programs and Technologies on DIB Unclassified Networks and Information Systems
#3: Reform the Department's Business Practices for Greater Performance and Affordability	3.1 Improve and strengthen business operations through a move to DoD-enterprise or shared services; reduce administrative and regulatory burden	Innovate for Competitive Advantage	Deliver a DoD Enterprise Cloud Environment to Leverage Commercial Innovation
		Optimize for Efficiencies and Improved Capability	Shift from Component-Centric to Enterprise-Wide Operations and Defense Model
			Optimize DoD Data Centers
			Optimize DoD Office Productivity and Collaboration Capabilities (ECAPS Capability Set 1)
			Optimize DoD Voice & Video Capabilities (ECAPS Capability Sets 2 & 3)
			Improve IT Category Management
			Improve Rapid Technology Deployment Processes
			Strengthen IT Financial Management Decision Making and Accountability
		Evolve Cybersecurity for an Agile and Resilient Defense Posture	Protect Sensitive DoD Information and Critical Programs and Technologies on DIB Unclassified Networks and Information Systems
			Reform DoD Cybersecurity Risk Management Policies and Practices

Mapping of DMS Goals and Objectives to NDBOP Goals and Objectives Management Committee (cont'd)

FYs 2018-2022 NDBOP Goals	NDBOP Objective	FY 2019 DMS Goals	DMS Objectives
#3: Reform the Department's Business Practices for Greater Performance and Affordability	3.3 Undergo an audit, and improve the quality of budgetary and financial information that is most valuable in managing the DoD	Optimize for Efficiencies and Improved Capability	Strengthen IT Financial Management Decision Making and Accountability

LEGEND

AI Artificial Intelligence

AISR Airborne Intelligence, Surveillance, and Reconnaissance

DIB Defense Industrial Base

DISN Defense Information Systems Network

DT Data Transport

ECAPS Enterprise Collaboration and Productivity Services

ICAM Identity, Credential, and Access Management

Source: The DoD OIG.

Management Comments

DoD Chief Information Officer

CHIEF INFORMATION OFFICER

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

MAY 23 2024

MEMORANDUM FOR INSPECTOR GENERAL OF THE DEPARTMENT OF DEFENSE
(ATTN: AUDITS – CYBERSPACE OPERATIONS)

SUBJECT: Review and Comment of DoD Inspector General Draft Report "DoD's Development and Maintenance of the Digital Modernization Strategy (Project No. D2023-D000CT-0115.000)

This is the Department of Defense Chief Information Officer (DoD CIO) comments on the review of the subject DODIG Draft Report. DoD CIO "agrees" with the Draft Report and provides to following comments:

DODIG RECOMMENDATION 1: We Recommend that the DoD Chief information Officer:

a. Develop and implement standard operating procedures that include, at a minimum:

i. Definitions for specific, verifiable, and measurable;

ii. Steps for reviewing the Digital Modernization Strategy annually alongside the DoD's Annual Performance Plan to determine if there are any performance gaps or changes to mission needs, priorities, or goals;

iii. Steps for documenting actions taken to address performance gaps between the Digital Modernization Strategy and the DoD's Annual Performance Plan.

iv. Steps for documenting their annual reviews, such as including a signature date on the Digital Modernization Strategy, and;

v. Requirements for the Governance Boards to maintain and submit documentation to the Office of the Chief Information Officer designee to support closure of the strategy elements.

b. Direct an official from the Office of the Chief Information Officer to review the 54 strategy elements that we determined are not specific, verifiable, and measurable (once the DoD Chief Information Officer has issued approved definitions for specific, verifiable, and measurable), and:

i. Revise the 37 strategy elements that are not closed to make them specific, verifiable and measurable, and;

ii. Determine whether adequate support exists to substantiate the completed status for the 17 remaining strategy elements and, if not, reopen and revise the strategy elements to be specific, verifiable, and measurable.

DoD Chief Information Officer (cont'd)

c. **Direct an official from the Office of the Chief Information Officer to revalidate that the mission needs, priorities, and goals of the Digital Modernization Strategy map to the current DoD Agency Strategic Plan and update the Digital Modernization Strategy accordingly.**

d. **Designate an official from the Office of the Chief Information Officer to oversee the development and maintenance of the Digital Modernization Strategy updates.**

DoD CIO Response: DoD CIO "agrees" with the DoD IG recommendation(s). DoD CIO is in the process of finalizing and coordinating the replacement of the former Digital Modernization Strategy (DMS) with a new strategy now known as Fulcrum: The Department of Defense Information Technology Advancement Strategy. The "Fulcrum" strategy features four lines of effort (LOE), 15 objectives, and 72 key results that are specific, measurable, achievable, relevant and timebound. North Dakota State University (NDSU) best practices for SMART Goal setting for Strategic Planning published July 2023 were utilized for the development of Fulcrum OKRs (see the NSDU website at: ndsu.edu/agriculture/extension/publications/goal-setting-strategic-planning). Following the "Fulcrum" publication, tentatively scheduled for July 2024, the legacy DMS including the objectives and key results (OKRs) will be sunset and replaced with the Fulcrum OKRs. Internal controls will be implemented in accordance with OMB Circular A-123 to ensure "Fulcrum" is administered in accordance with OMB Circular A-130. The DoD CIO has taken the following action to pursue all recommendation(s) in some form.

- DoD CIO directed the Deputy Chief Experience Officer (DCXO), [redacted], to develop and implement standard operating procedures (SOP) to ensure the application of SMART goal setting for strategic planning. Procedures will include an annual strategic review comparing both the DoD Annual Performance Plan and Fulcrum to address potential changes and impacts to mission needs, priorities, goals, and objectives. Additionally, procedures will document actionable steps to address gaps and memorialize annual review completion with designated signatories. The expected completion date for this action is August 30, 2024.

- DoD CIO established the DoD Strategic Action Group October 27, 2023 (Chaired by the PDCIO but not chartered), which currently serves as the governing council for past DMS strategy elements and future Fulcrum OKRs.

- DoD CIO directed the DCXO, [redacted], to facilitate the review of 54 identified DMS strategy elements (see attached). Specifically, the revision of 37 open elements applying SMART goal setting and substantiation of 17 closed elements as complete. If element completion for any is indeterminable each will be reopened, and SMART goal setting will apply. All 54 elements will be cross walked against new Fulcrum OKRs for applicability, SMP performance monitoring, and sunsetting if warranted. The expected completion date for this action is September 27, 2024.

DoD Chief Information Officer (cont'd)

Fulcrum describes "what" the DoD must achieve with respect to advancing IT for the Warfighter and "why" it matters. The detailed implementation plan required to achieve these goals and objectives will describe the "how" we will get there. It is forthcoming as part of our immediate next steps. The attached Fulcrum DOD IT Advancement Strategy Overview (abridged) provides a demonstrated alignment of Fulcrum LOE with the DoD Strategic Management Plan Priorities.

- DoD CIO designated the DCXO, [redacted], to oversee and administer the development and maintenance of Fulcrum, the replacement for DMS.

A security review was conducted of the Draft Report with concurrence and no changes made to the CUI sensitivity and control marking of the document/report.

The DoD CIO points of contact for this matter are [redacted], DoD CIO Audits LNO, [redacted], and [redacted], DoD CIO DCXO, [redacted]

Hon. John B. Sherman

Attachments:
As stated

3

Acronyms and Abbreviations

CIO	Chief Information Officer
DCXO	Deputy Chief Experience Officer
DMS	Digital Modernization Strategy
IRM	Information Resource Management
IT	Information Technology
JAIC	Joint Artificial Intelligence Center
NDBOP	National Defense Business Operations Plan
OCIO	Office of the Chief Information Officer
OMB	Office of Management and Budget


INSPECTOR GENERAL
INTEGRITY
EFFICIENCY
DEPARTMENT OF DEFENSE

Whistleblower Protection
U.S. Department of Defense

Whistleblower Protection safeguards DoD employees against retaliation for protected disclosures that expose possible fraud, waste, and abuse in Government programs. For more information, please visit the Whistleblower webpage at www.dodig.mil/Components/Administrative-Investigations/Whistleblower-Reprisal-Investigations/Whistleblower-Reprisal/ or contact the Whistleblower Protection Coordinator at 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; 703.604.8324

www.twitter.com/DoD_IG

LinkedIn
www.linkedin.com/company/dod-inspector-general/

DoD Hotline
www.dodig.mil/hotline

DEPARTMENT OF DEFENSE | OFFICE OF INSPECTOR GENERAL

4800 Mark Center Drive
Alexandria, Virginia 22350-1500
www.dodig.mil
DoD Hotline 1.800.424.9098