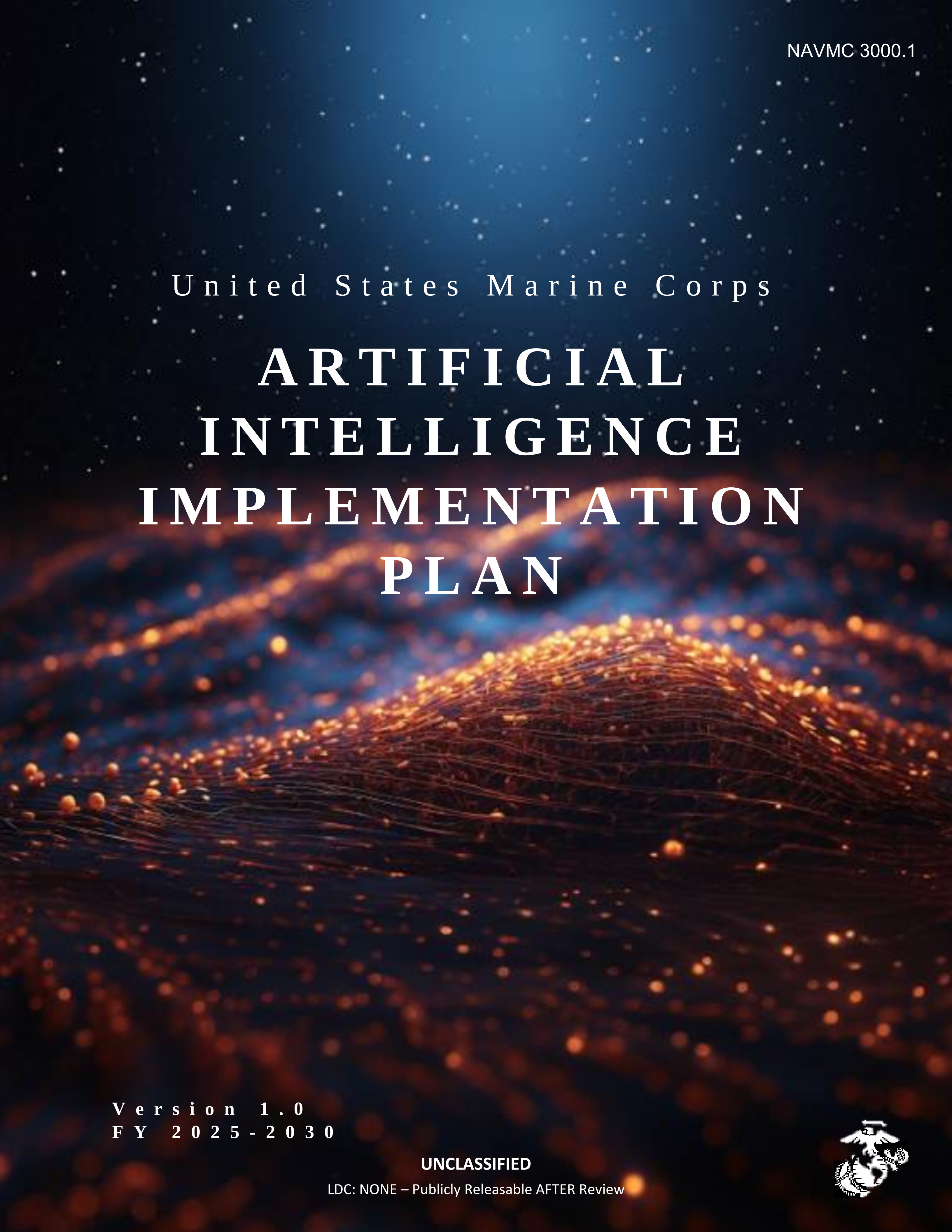


NAVMC 3000.1

United States Marine Corps

ARTIFICIAL INTELLIGENCE IMPLEMENTATION PLAN

Version 1.0
FY 2025-2030

UNCLASSIFIED

LDC: NONE – Publicly Releasable AFTER Review

05
MARINES
108

Prepared by

Christopher D. Clark, Capt, DC I SDO, USMC 20250423

NAME **Date**

Reviewed by

Dr. Colin Crosby, DC I SDO, USMC 20250423

NAME **Date**

Approved by

Melvin G. Carter
Lieutenant General, U.S. Marine Corps
Deputy Commandant for Information M.G. Carter 20250423

NAME **Date**

PCN: 10048006900

Record of Amendments

VERSION	DATE	CHANGES
0.1	07/25/2024	Initial Draft
0.2	08/21/2024	AI Working Group feedback incorporated
0.3	09/18/2024	AI Working Group round 2 feedback incorporated
0.4	10/16/2024	AI Working Group round 3 feedback incorporated
0.5	11/22/2024	AO level feedback incorporated via DON-241031-WFHX
0.6	01/22/205	O6/GS15 level feedback incorporated via DON-241216-9QRF
0.7	02/21/2025	O6/GS15 round 2, internal DC I staffing feedback incorporated
0.8	03/28/2025	GO/FO/SES level feedback incorporated via DON-25030354RZ
0.9	04/23/2025	Final revisions

TABLE OF CONTENTS

Executive Summary

The United States Marine Corps (USMC) recognizes artificial intelligence (AI) as a transformative technology to enhance decision advantage in the evolving landscape of modern warfare. The USMC AI Implementation Plan (AI IPlan) was developed in response to the publication of the USMC AI Strategy[1] as a critical component of executing the 39th Commandant's Planning Guidance to leverage "advances in artificial intelligence to enhance decision making at the tactical edge."[2] This plan aligns with key directives, including those outlined in Force Design[3], the Department of the Navy (DON) Data and AI Weaponization Strategy under development, the Department of Defense (DoD) Data Analytics and AI Strategy[4], and the Executive Order 14179 on AI.[5]

Purpose: The AI IPlan identifies the actions, offices of primary responsibility (OPRs), and milestones for the implementation of the USMC AI Strategy. It establishes a Digital Transformation Pilot (DXP) project as a near-term vehicle for implementation and to gauge and measure success. The plan is designed as an integrating document that aligns activities to achieve unity of effort. Building upon strategic directives, it identifies clear tasks associated with each goal and objective.

Scope: This document is applicable to the Marine Corps Total Force, with the Fleet Marine Force as the primary customer.

Approach

1. Digital Transformation Pilot: Digital transformation is the process of adopting and implementing digital technology to increase value through innovation and efficiency. This plan establishes a Digital Transformation Pilot project that will deploy Digital Transformation Teams (DXTs) to support and measure successful implementation. This pilot will focus on the following:

- Delivery of digital, data, analytics, and AI solutions.
- Delivery of process optimizations.
- Advise the command on opportunities and risk of digital, data, and AI employment.
- Validate existing processes and identify opportunities for data and AI integration.
- Reporting via data and AI governance structures for Service alignment and decisions.

2. Data as the Foundation for AI: Data management, governance, and architecture are essential for effective AI implementation. This plan supports and informs the ongoing strategic efforts to update the USMC Data Implementation Plan (DIP) and outlines inclusion of inspectable items to be introduced into the Commanding General's Inspection Program to shift the culture toward data-driven decision.

3. AI Infrastructure: An AI infrastructure operations planning team (OPT) will identify the requirements for storage & compute, resource management, development security operations (DevSecOps) machine learning operations (MLOps) environments, and ML platforms for enterprise and tactical employment, with cybersecurity incorporated throughout.

4. Workforce: This plan proposes changes to the workforce that are required to support the data and AI strategic goals. There are three primary workforce groups critical to AI implementation:

- Marines who utilize AI capabilities to enhance operational effectiveness.
- Workforce that builds, maintains, and refines digital, data, and AI solutions.
- Leadership charged with making risk decisions on the use of AI and AI-enabled systems.

5. Training and Education: Appropriate training and education will support the workforce to ensure mission success. This includes:

- Immediate education opportunities developed and made available to upskilling the workforce.
- AI training and education developed and institutionalized to support the AI workforce and the Total Force.

6. Policies and Policy Blockers: The Marine Innovation Unit (MIU) conducted an assessment with recommendations on potential existing roadblocks to AI implementation. They highlight the following areas for consideration:

- The authority to operate (ATO) process.
- Existing risk management framework.
- Fragmented data management across the Service.
- Cultural approach to build, deploy, and manage software.

7. USMC Center for Digital Transformation: An assessment will be conducted on establishing a USMC Center for Digital Transformation (CDX). The CDX will provide digital, data, and AI knowledge-based products designed to support and grow a healthy ecosystem, developer community, and user base. The center will accelerate the fielding of emerging technologies, including AI, across the Service via strong connections with industry and academia.

8. AI Governance: AI Governance ensures compliance, resource alignment, Responsible AI support, while encouraging innovation. The plan tasks the Service Data Office (SDO) with establishing AI governance by identifying integration opportunities with current governance entities across the USMC enterprise landscape.

9. Resource Framework: The plan describes how resources will be aligned across the Service for effective AI implementation and oversight to support enterprise-to-edge capabilities for current and future requirements.

Execution

Tasks and OPRs are listed to facilitate effective implementation. Each task contains anticipated key performance indicators (KPIs), while charging the OPR to refine their KPIs following the publication of this plan. OPRs will report task execution progress to the AI Working Group (AIWG) on a quarterly basis. Figure 1 provides a high-level overview of the implementation timeline and milestones.

The AI IPlan is a detailed roadmap to accomplish the USMC AI Strategy[1] by charting the course to evolve the Marine Corps into an AI-enabled Force, ready to confront the challenges of future conflicts with enhanced readiness and effectiveness. It is a testament to the Corps' dedication to maintaining a competitive edge through the responsible and innovative use of AI technology.

Implementation Timeline

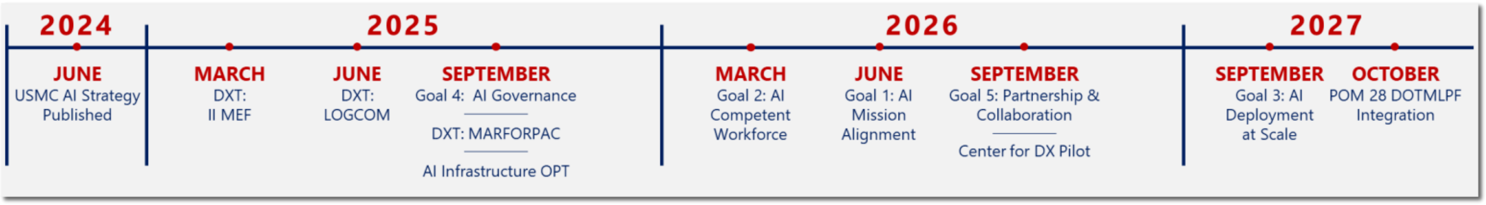

2024
JUNE
USMC AI Strategy Published
2025
MARCH
DXT: II MEF
JUNE
DXT: LOGCOM
SEPTEMBER
Goal 4: AI Governance
DXT: MARFORPAC
AI Infrastructure OPT
2026
MARCH
Goal 2: AI Competent Workforce
JUNE
Goal 1: AI Mission Alignment
SEPTEMBER
Goal 5: Partnership & Collaboration
Center for DX Pilot
2027
SEPTEMBER
Goal 3: AI Deployment at Scale
OCTOBER
POM 28 DOTMLPF Integration

Figure 1. USMC Artificial Intelligence Implementation Plan milestones and timeline.

1. Introduction

In the rapidly evolving landscape of modern warfare, leveraging information effectively is crucial for the success of the Marine Corps across all domains and warfighting functions. This AI IPlan stands as a strategic blueprint to mature the Service into a 21st Century fighting force that innovates and integrates AI into warfighting functions and business processes.

The AI IPlan outlines actionable and measurable tasks for the Service to adopt, leverage, and integrate AI. It addresses mission alignment, scalable deployment, Responsible AI governance,[6] and strategic partnerships and collaboration—all aimed at empowering the most critical component: the Marines that will harness this technology to accomplish their mission. By aligning with Force Design,[3] the Department of the Navy (DON) Data and AI Weaponization Strategy under development, the DoD Data, Analytics, and Artificial Intelligence Adoption Strategy,[4] and Executive Order 14179[5] on AI, the USMC AI IPlan provides a structured framework for implementing these strategies.

1.1 Purpose

This AI IPlan identifies the actions required to realize the USMC AI Strategy[1]. It is designed to be an integrating document that will align activities to achieve unity of effort. Building upon the strategic directives outlined, this implementation plan identifies clear lines of effort aligned with specific goals and objectives.

In addition to task development, this document addresses resource alignment in Appendix B, requirements generation in Appendix C, risk management in Appendix F, and stakeholder engagement to ensure that all facets of the implementation process are executed and measured. By doing so, it lays the groundwork for the successful integration of AI technologies across various Marine Corps functions and operations.

1.2 Problem Statement

Data management is a significant challenge facing AI implementation in the Marine Corps, and the current data climate will prove a challenge for developing and scaling AI solutions. AI technology continues to evolve rapidly, creating opportunities for the Service in the areas of doctrine, organization, training, materiel, leadership and education, personnel, facilities, and policy development (DOTMLPF-P). In alignment with the ongoing parallel efforts to address the inherent data challenges, this plan will focus on:

1. Misalignment of AI with mission objectives
2. Growing gaps in AI competency
3. Difficulty deploying AI at scale from the enterprise to the tactical edge
4. Legacy governance frameworks that stifle innovation
5. Barriers to collaboration and partnerships

A clear implementation roadmap will advance AI capabilities by realigning AI initiatives with mission objectives, enhancing AI training and education programs, streamlining governance to fosters innovation, and expanding collaborations.

1.3 USMC AI Operational Discussion

I MEF, supporting Indo-Pacific Command, operates with over 50,000 Marines dispersed across vast maritime and littoral regions. In this environment, timely intelligence and effective decisions are paramount, yet complicated by distributed data, contested electromagnetic spectra, and limited bandwidth. Advanced AI capabilities could transform how I MEF plans and executes missions.

I MEF Capabilities Enhancement Vignette

> *In a forward command post, Marines employ AI-enabled capabilities to analyze multilingual intercepts, sensor data, and satellite imagery in seconds. Language processing AI systems assist in producing concise summaries for decision-makers while computer vision systems augment analysts in identifying enemy locations and movements to accelerate the kill chain, allowing commanders to focus on operations rather than receiving information overload.*
>
> *As adversarial jamming and delayed shipments cause conditions to shift, a logistics officer leverages predictive analytics with reinforcement learning to continuously adjust supply routes to keep critical materiel flowing. Marines leverage their training and judgment, affirming or rejecting AI-generated content to ensure each action aligns with mission intent.*
>
> *Accessible data, hardened edge computing, and emissions-controlled processing are only a few of the components needed for AI integration in contested networks. Engineers will need to monitor and continuously train models under degraded conditions to ensure predictions are relevant and accurate. Leaders, fully aware that AI can magnify both success and failure, ensure processes and procedures are in place for the responsible use of AI before execution.*
>
> *Marines leverage AI to enhance their ability to sense, decide, and act in complex environments. By weaving advanced technologies into daily operations, I MEF can enhance speed, precision, and resilience, to turn uncertainty into decisive action.*

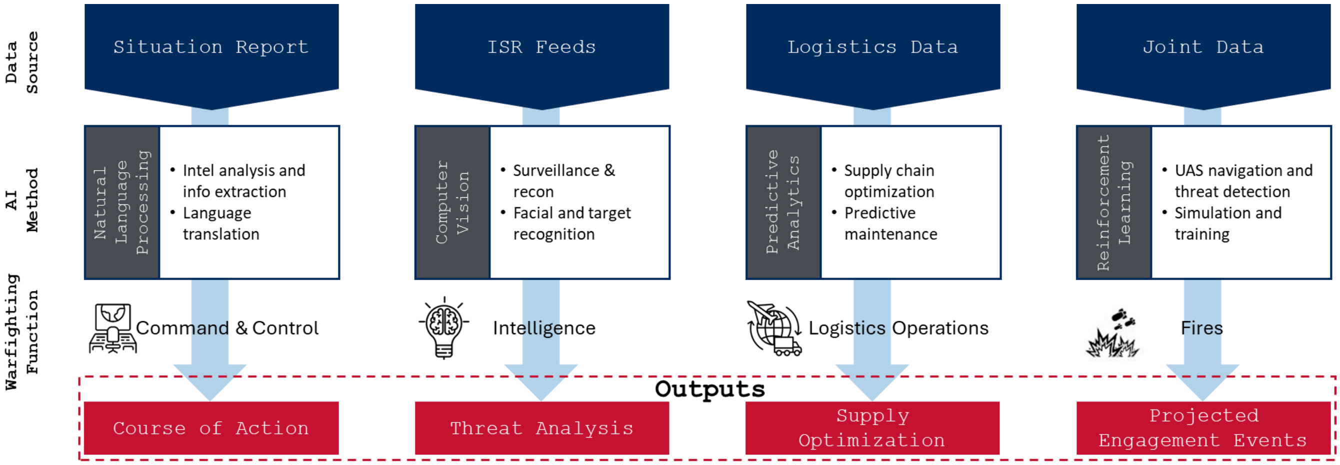


Figure 2. Example information flow for the USMC AI Operational Vignette.

While this vignette explores how AI can shape operations within I MEF, a similar vignette can be developed for II MEF, III MEF, and other commands across the Marine Corps. This vignette exemplifies the interdisciplinary nature of AI, the importance of a workforce that understands building trustworthiness in data processing methods in pursuit of AI to reshape the battle space.

1.4 Scope

This AI IPlan is applicable to the Marine Corps Total Force with the Fleet Marine Force as the primary customer. It should be leveraged as a core document to align resources and activities.

2. Operational Imperative

The USMC AI Strategy presented a vision to empower Marines with advanced AI capabilities to support decisive information advantage. This document operationalizes that vision by laying out the necessary actions. The AI Strategy is the driving force that underpins the activities presented in this AI IPlan. The operational imperative to achieve success hinges on the execution of these activities.

2.1 Guiding Principles

The following guiding principles support the integration of AI across the Service.[1] AI is a cross-functional technology that impacts critical systems and infrastructure, autonomous vehicles, cyber-physical systems, IT services, mission planning, imagery analysis, and much more. These guiding principles can be applied to the integration of AI across this diverse landscape:

1. **Accelerate** the integration of AI to provide reliable insights for enhanced decision-making and operational effectiveness, in accordance with the DoD's Responsible AI principles.[7]

2. **Empower** Marines with the knowledge, skills, and tools to rapidly implement AI. This requires developing a workforce proficient in AI and unleashing them to be innovative in seeking novel solutions for existing and future challenges.

3. **Grow** an AI workforce able to oversee, adopt, and integrate AI capabilities.

4. **Set conditions and requirements** to ensure data is visible, accessible, understandable, linked, trustworthy, interoperable, and secure (VAULTIS).[4]

5. **Build and strengthen** strategic partnerships to accelerate adoption, foster innovation, and enhance interoperability with academia, industry, Joint, and mission partners.

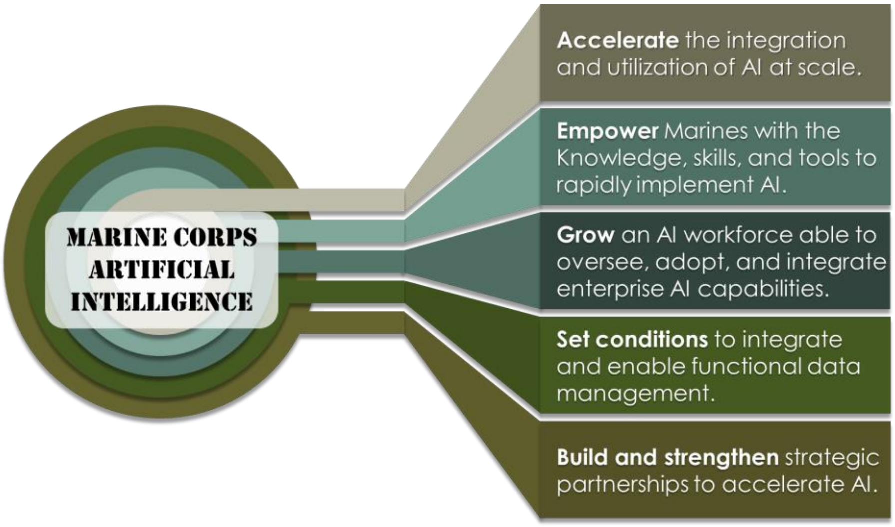

MARINE CORPS ARTIFICIAL INTELLIGENCE
Accelerate the integration and utilization of AI at scale.
Empower Marines with the Knowledge, skills, and tools to rapidly implement AI.
Grow an AI workforce able to oversee, adopt, and integrate enterprise AI capabilities.
Set conditions to integrate and enable functional data management.
Build and strengthen strategic partnerships to accelerate AI.

Figure 3. Guiding principles supporting Marine Corps Artificial Intelligence.

3. Approach

This section outlines the components that support the AI IPlan in achieving the USMC AI Strategy goals and objectives.[1] Each activity requires that the OPRs develop project plans and revise key performance indicators (KPIs) to support progress reporting and measure successful implementation. Information about progress reporting expectations will be outlined through additional correspondence following the publication of this plan.

3.1 Digital Transformation Pilot Project

Digital transformation is the process of adopting and implementing digital technology to increase value through innovation and efficiency.[8] It makes data a strategic asset by which analytics and AI can be leveraged. Digital transformation is the holistic approach necessary for effective AI implementation, to ensure mission alignment, and avoid the *solution in search of a problem* dilemma by identifying solutions that are simple, effective, understandable, and affordable versus pursing unnecessary and overly complex AI solution. Digital transformation is an enduring action, and the Marine Corps will continue to digitally transform the Service for the foreseeable future.

The Marine Corps will establish Digital Transformation Teams (DXTs) via the Digital Transformation Pilot (DXP) project as the immediate vehicle for this plan. The DXP supports implementation through the following:

- Provide commands with integrated digital capabilities by digitizing and optimizing processes, establishing robust data pipelines, delivering advanced analytics, and implementing AI-driven solutions that enhance operational effectiveness.
- Advise commanders and their staff on opportunities and risk associated with AI employment.
- Validate existing processes for technology integration and assess the effectiveness and scalability of digital solutions.
- Provide, at a minimum, a quarterly brief and report to the AI Working Group (AIWG) on critical opportunities and challenges related to data and AI implementation.

DXTs will play an essential role in transforming the Service into a data-centric organization that can leverage cutting edge digital and AI capabilities. DXTs will utilize the AI and analytical maturity model (AIAMM) in Appendix J as a starting point to understand the command's level of maturity to aid the focus of efforts and resources appropriately.

The DXP will support the Service in driving the DOTMLPF-P process for institutional change. The DXP takes the holistic vision of the USMC AI Strategy,[1] and the implementation approach of this document, and focuses it on achieving immediate results to solve current mission problems and provide critical feedback that informs Service-level decisions.

Details of the DXP is provided in Appendix A, allowing for a modular and scalable implementation across a large and diverse enterprise.

3.2 Data as the Foundation for AI

Data is the foundation for analytics and AI. The Service Data Office (SDO) is actively updating the DIP[9] to address existing data challenges that include data lifecycle management, data quality and governance, and a scalable and robust data architecture.

1. **Data Lifecycle Management**
   A robust framework that covers every stage of data from generation, storage, transformation, to serving. Lifecycle management ensures that AI models are developed and trained on quality data that continuously flows through the system.

2. **Data Quality and Governance**
   Provides the framework that ensures data is clean, complete, accurate, and compliant with policy and regulations. Robust data governance and security measures are essential to protect sensitive information and maintain high data quality for reliable AI models.

3. **Scalable and Robust Data Architecture**
   A scalable and resilient data architecture is key to managing and protecting the enterprise data environment. Aligned with zero trust principles,[10] this architecture streamlines the development, security, and operations pipelines. Along with data lifecycle management and data governance, an adequate data architecture is essential to achieve VAULTIS[4] principles. As a hybrid multi-cloud organization, a data architecture for managing data silos and promoting a micro-service-based ecosystem is critical to access the large quantities of data needed to develop AI models and to conduct continual learning through the model lifecycle. As technology changes rapidly, data architectures must maximize flexibility and maneuverability.

4. **Managing Change**
   Implementing this framework involves significant transformation that may encounter resistance to change, potentially stifling innovation. Effective change management, as detailed in Appendix E, is therefore critical. It will ensure broad organizational adoption and support the development, deployment, and scalability of AI solutions in a secure, efficient manner.

This integrated approach—treating all data with strategic importance and explicitly addressing warfighting data with maturity—outlines the core data requirements for reliable, innovative AI solutions that enhance both enterprise analytics and operational capabilities.

3.3 AI Infrastructure

A well-designed enterprise AI infrastructure is critical to accelerate the development, deployment, and integration of AI-enabled capabilities within the USMC. The infrastructure provides the foundation on which data-driven technologies are built. With AI rapidly influencing strategic, operational, and tactical decision-making, it is paramount to have reliable systems that can handle the complexities of modern challenges. The infrastructure must support government application development, adopting Joint Services solutions, and integrating industry software.

1. **Storage and Compute**
    - AI models require large volumes of data and substantial processing power for training and inference. Well-planned infrastructure that can scale these resources on demand is essential for mission success.

2. **Development Environment**
    - A secure, integrated development environment is needed to unify DevSecOps and MLOps.
    - This environment must support code development, continuous integration and continuous development, testing, and deployment, while managing the machine learning lifecycle from model training and validation to deployment and monitoring.

3. **Resource Management**
    - Efficient resource management must ensure resources for AI workloads are optimized and available to the right teams at the right times.

4. **ML Platform**
    - A unified ML platform is needed to consolidate data management, model training, experimentation, and deployment into a supportable ecosystem.
    - An ML platform must include tools to support model development, model stores, feature stores, and vendor integrations.

What is cutting edge today will be legacy tomorrow. It is essential that AI infrastructure is both flexible, reversible, and loosely coupled to support maneuverability as technology advances.

3.4 Workforce

Successful adoption requires proliferation of digital and AI skills throughout the Total Force and upskilling specialized Marines who can solve complex data, analytics, and AI challenges. There are three primary groups critical:

- Marines who utilize AI capabilities to enhance operational effectiveness.
- The AI workforce that builds, maintains, and refines advanced digital and AI solutions
- Leadership charged with making risk decisions on the use of AI.

Marines are not passive users of these systems. Instead, they must understand the system's capabilities and limitations, recognizing when outputs are incorrect and understanding their right and left lateral limits. Leaders must understand the full scope of the risk associated with the use of AI systems to make mission critical decisions.

To accomplish this, comprehensive AI training and education is being developed. This will integrate with existing programs to train and educate Marines in AI and AI-related fields, ensuring Marines are appropriately skilled and resourced to accomplish their mission. Marines will continue to digitize processes, support and enforce data standards, and effectively utilize AI systems.

3.5 AI Workforce Supported by Digital Operations

Effect development and use of AI systems requires upskilling specialized Marines who can solve complex data, analytics, and AI challenges. Marines that conduct digital operations provide the critical foundation upon which AI initiatives are built and sustained, creating the digital ecosystem necessary for effective AI integration.

Central to this approach is assessing the development of a series of military occupational specialties (MOSs) to provide career paths for future data and AI workforce Marines. These career paths would produce Marines skilled in software development, data analytics, process optimization, and AI systems. These Marines will digitize analog processes, manage data pipelines, and develop AI-enabled solutions. Embedding digital operations capabilities within operational units ensures digital transformation remains aligned with mission needs and operational realities. In addition, near-term training opportunities, such as a formalized AI training and education will be prioritized to ensure Marines in leadership roles and technology-driven MOSs have foundational AI knowledge.

The Marine Corps Software Factory (MCSWF) is one approach to provide MOS governance, standards, and operational support for digital and AI initiatives across the Marine Corps. It has the potential to serve as a hub for advanced capabilities, skill standardization, and best practices, to ensure consistency and quality Service-wide. This training pipeline includes AI-specific modules and specialized AI tracks, to ensure Marines understand AI fundamentals and can focus on AI development and implementation.

The Marine Corps Tactical Systems Support Activity (MCTSSA) Digital Solutions Branch is a mission-funded software development team with experience in development and delivery of AI solutions to the Service. MCTSSA is one of few organizations in the Marine Corps postured to engage in cooperative research and development agreements with industry partners, exposing Marines to industry leading experts and technology. The Office of Naval Research designation as a technical activity and the Department of Defense designation as a science and technology reinvention laboratory postures MCTSSA to develop government owned AI solutions, provide essential support to the Digital Transformation Pilot, and support MCSWF-trained software developers as they grow through their Marine Corps career.

Through institutionalizing digital operations, the Marine Corps will create a sustainable, adaptive capability to enable current and future AI technologies. The path to effective AI integration depends on digital operations.

3.6 USMC Center for Digital Transformation

A USMC Center for Digital Transformation will contribute to developing knowledge-based products such as policy, guidance, standards, and best practices. These are critical to support a healthy ecosystem, developer community, and a strong user base. This organization will deliver knowledge-based products necessary to maintain pace with AI advancements and other emerging technologies. It will directly enhance AI initiatives by accelerating the work necessary for agile software delivery.

In addition to knowledge-based support, the Center for Digital Transformation will deliver advanced technological solutions rapidly and effectively across the Service. It will support the Digital Transformation Teams and integrate with digital operations by providing a focused structure designed to speed discovery, testing, prototyping, and fielding of emerging capabilities. By fostering close collaboration with partners, like the Naval Postgraduate School (NPS), the Marine Corps University, and the Marine Corps Warfighting Laboratory Science & Technology (MCWL S&T), the USMC Center for Digital Transformation will leverage academic expertise, research talent, and cutting-edge technical resources to ensure innovations are not siloed, duplicative, or delayed.

The program addresses several Force Design imperatives:

- Accelerated AI adoption for tactical decision advantage.
- Enhanced information warfare capabilities.
- Improved stand-in force effectiveness.
- Strengthened technical talent development.
- Rapid capability deployment to the Fleet Marine Force.

Success metrics focus on operational impact, technical feasibility, and resource efficiency. Each phase must include clear deliverables and exit criteria, ensuring responsible progression from concept to deployment.

Additional aspects of the USMC Center for Digital Transformation will include model development, data and model cataloging, and the deployment of highly specialized teams to assist the Digital Transformation Teams in identifying and delivering challenging solutions.

The DC I, SDO will conduct a feasibility of support assessment for standing up a USMC Center for Digital Transformation.

3.7 AI Governance

The DC I, SDO has been designated as the office responsible for policy, governance, and oversight for Marine Corps AI to inform requirements for providing AI to the Service.[1] The AIWG, chaired by the SDO, is the Service-level body for AI governance[11] that provides alignment of policy, resourcing decisions, and ethical and Responsible AI principles impacting the Marine Corps Total Force. The AIWG is a significant foundation, and additional governance processes and structure will be developed and implemented via this plan.

3.8 Policies and Policy Blockers

In development of the AI IPlan, MIU was asked to assess roadblocks potentially limiting AI implementation. The assessment in Appendix H provides an overview of the current landscape and recommended policy changes for effective implementation. Digital technologies are notoriously fast-moving and becoming increasingly integrated in the private sector. Appendix H provides an assessment of the limitations of the Marine Corps' current posture toward emerging technologies with recommended actions that includes following topics:

1. The ATO Process
2. The Existing Risk Management Framework (RMF)
3. Fragmented Data Management Across the Service
4. Cultural Approach to Build, Deploy, and Manage Software

By addressing these challenges via Task 4.2.1, the Marine Corps can more effectively shape AI-solutions to support emerging use cases. This narrative examines the steps needed for the Marine Corps to become a smart adopter and user of AI technology, harnessing its potential to drive operational improvements, enhance situational awareness, and inform decision-making, while collaborating with industry and academia to remain current with the latest AI advancements.

3.9 Resourcing Alignment

AI is cross-cutting and touches many programs, applications, and disciplines. Appendix B outlines the resourcing framework to align AI technology, while Appendix C outlines existing requirements that align to several objectives in this implementation plan. A gap analysis is necessary following the publication of this plan to ensure new gaps that manifest as a result of this plan are identified, included in the annual gap list, and written into requirements. The total collection of requirements aligned to this document support the resource funding essential to this implementation.

4. Execution

4.1 Roles, Responsibilities, and Progress Reporting

The implementation of this plan depends on actions from across the Service. Coordination was conducted at the General Officer level with full concurrence of this plan as identified in Appendix K. This coordination supports the OPR assignments needed to achieve the strategic goals of the USMC AI Strategy. OPRs are responsible for reporting progress and challenges to the AIWG on a quarterly basis. Reporting templates will be coordinated following the publication of this plan.

Roles and responsibilities:

- DC I, SDO: Oversight authority and responsibility to ensure the implementation is on track and to report progress to the DC Information. Overall accountable for the execution of this AI IPlan.[12]

- AIWG: Service-level cross-functional body responsible for AI governance[11] and coordination to facilitate achieving the objectives and tasks outlined in this AI IPlan. The AIWG will provide recommendations to the next echelon as appropriate.

- OPRs: Responsible for the overall accomplishment of their assigned objectives and associated tasks.

4.2 Goals, Objectives, and Tasks

This section delineates the strategy for implementing AI by breaking down goals into constituent objectives and tasks. For every objective, an OPR is designated to be responsible to the SDO for the successful completion of the assigned tasks for coordination.

The responsibilities of the OPR include the following elements:

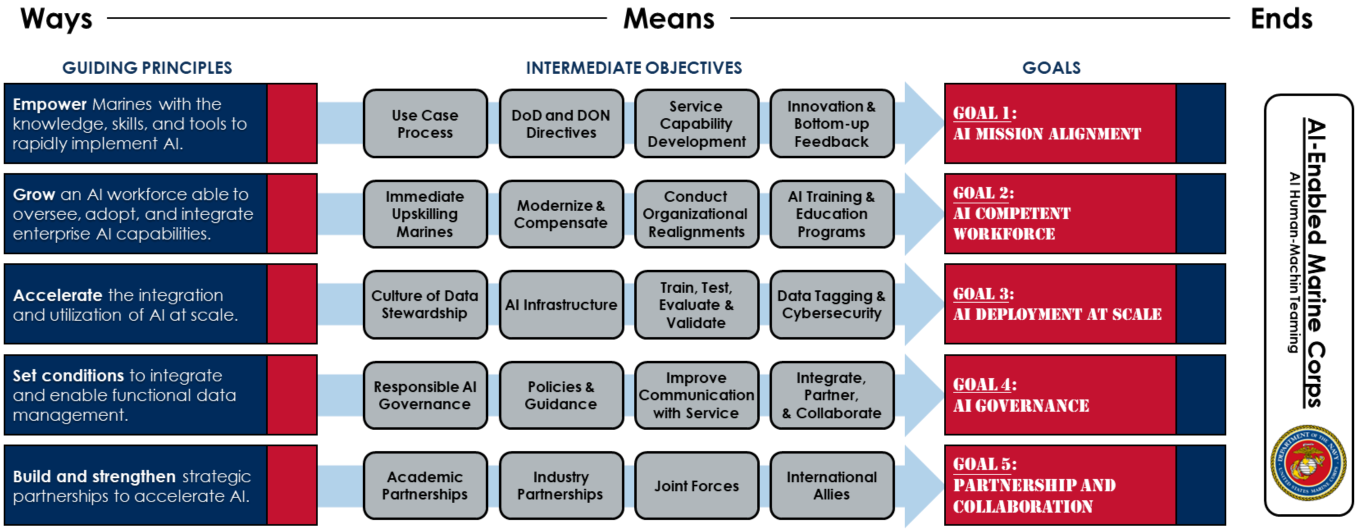
1. Plan of Action and Milestones: Developing a plan of action that lists the steps to achieve the objective. This will include specific milestones as checkpoints to measure progress against the plan. The milestones should be time-bound and achievable, ensuring that the strategy stays on track.

2. Task Prioritization: Prioritization for resource allocation to ensure critical objectives are addressed first. This will streamline efforts and focus attention where it is most needed.

3. Identification of Risks and Challenges: Identifying potential risks and challenges that could hinder the achievement of objectives related to technological constraints, resource constraints, cultural barriers, and interoperability issues.

Progress updates will be provided to the AIWG on, at least, a quarterly basis. This will include changes to implementation timelines and identification of unnecessary program duplication and associated mitigation actions.

The following section identifies objective-level OPRs, provides a high-level view of key tasks, and outlines the associated timelines. These tasks are the building blocks to implement and adopt AI effectively, while posturing the Service for emerging technological breakthroughs and advancements.



GUIDING PRINCIPLES	INTERMEDIATE OBJECTIVES				GOALS
Empower Marines with the knowledge, skills, and tools to rapidly implement AI.	Use Case Process	DoD and DON Directives	Service Capability Development	Innovation & Bottom-up Feedback	**GOAL 1:** **AI MISSION ALIGNMENT**
Grow an AI workforce able to oversee, adopt, and integrate enterprise AI capabilities.	Immediate Upskilling Marines	Modernize & Compensate	Conduct Organizational Realignments	AI Training & Education Programs	**GOAL 2:** **AI COMPETENT WORKFORCE**
Accelerate the integration and utilization of AI at scale.	Culture of Data Stewardship	AI Infrastructure	Train, Test, Evaluate & Validate	Data Tagging & Cybersecurity	**GOAL 3:** **AI DEPLOYMENT AT SCALE**
Set conditions to integrate and enable functional data management.	Responsible AI Governance	Policies & Guidance	Improve Communication with Service	Integrate, Partner, & Collaborate	**GOAL 4:** **AI GOVERNANCE**
Build and strengthen strategic partnerships to accelerate AI.	Academic Partnerships	Industry Partnerships	Joint Forces	International Allies	**GOAL 5:** **PARTNERSHIP AND COLLABORATION**

Figure 4. USMC Artificial Intelligence Strategic Implementation Framework

Strategic Goal 1:
AI Mission Alignment

Objective 1 - DoD Directives

- **Lead Department:** DC I
- **Timeframe:** End Date: NLT Feb 2026

- **Task: 1.1.1:** DC I, in coordination with Commander Marine Corps System Command (MCSC) and Program Executive Office Digital and Enterprise Services (PEO-DES), facilitate the development of a centralized enterprise portal on all relevant network enclaves to communicate, at a minimum, the following: Training and education resources, available AI capabilities, and AI policies and guidance.

Objective 2 - Service Capabilities

- **Lead Department:** Deputy Commandant for Combat Development and Integration (DC CD&I)
- **Timeframe:** Continuous

- **Task: 1.2.1:** DC CD&I, in coordination with DC I, continuously review urgent need statements across the Service and decompose them into capability requirements, transitioning them into requirement documents. Update key performance parameters, objective values, and threshold values based on the projected state-of-the-art capabilities, and develop standard requirements lexicon for use across programs and warfighting functions as applicable.

- **Task: 1.2.2:** DC CD&I, in coordination with acquisition communities, develop transition plans for initiatives that demonstrate high return on investment. Transition plans will apply the doctrine, organization, training, material, leadership and education, personnel, and facilities (DOTMLPF) for adoption of a capability over a pre-defined timeline

Objective 3 - Tactical Innovation

- **Lead Department:** DC I
- **Timeframe:** End Date: NLT May 2026

- **Task: 1.3.1:** DC I, in coordination with DC CD&I, develop a use case process that captures, assesses, and prioritizes concepts for the application of AI from across the warfighting functions, and at all echelons, to implement targeted actions. Through the collection of use cases, identify major roadblocks in policy, workforce, and infrastructure that have a large impact on innovation and acceleration of AI implementation to mitigate through change.

- **Task: 1.3.2:** DC I, oversee the establishment of the Digital Transformation Pilot as described in Appendix A to support commanders with implementing and incorporating digitization, data, analytics, and AI across their commands. Incorporate the Digital Transformation Teams into data and AI governance for resource alignment, oversight, and Service-level decisions.

Strategic Goal 2:
AI Competent Workforce

Objective 1 - Foundational Training and Education

- **Lead Department:** CG Training and Education Command (TECOM)
- **Timeframe:** End Date: NLT Mar 2026

- **Task: 2.1.1:** CG TECOM, identify available learning tools, resources, and current use-cases across the DoD and industry and centralize these resources into a repository for proactive learning, ensuring commanders and leaders are empowered to promote and authorize AI training.

- **Task: 2.1.2:** CG TECOM, identify costs and requirements for licensing external training resources outside of the USMC, while aligning with FMF capabilities and existing Programs of Records (PoRs) to enable shared funding and rapid acquisition to determine long term viability and funding.

Objective 2 - AI Talent Modernization

- **Lead Department:** DC I
- **Timeframe:** End Date: NLT Nov 2025

- **Task: 2.2.1:** Deputy Commandant for Manpower and Reserve Affairs (DC M&RA), analyze career retention compensation opportunities, to include, at a minimum, monetary, billet preference, established career-progression opportunities that support the development and retention of the AI workforce.

- **Task: 2.2.2:** DC I, develop and submit the concept prospectus that supports the Digital Operations Concept for consideration via the DOTMLPF process.

Objective 3 - AI-Ready Workforce

- **Lead Department:** DC I
- **Timeframe:** End Date: NLT Mar 2026

- **Task: 2.3.1:** DC I, implement and lead the Marine Corps Cyberspace Workforce Enterprise Program to expand development resources, such as the Information Development Institute, and bolster support for data analytics.

- **Task: 2.3.2:** DC M&RA, supported by DC I, ensure the information-related civilian workforce is included in AI workforce modernization. Analyze how to maximize return on investment in the civilian information-related workforce segment; methods to standardize the prediction of future civilian workforce needs; how to improve position descriptions; how to speed hiring; and how to make civilian workforce data more accessible for talent management initiatives.

- **Task: 2.3.3:** CG TECOM, develop and institutionalize the training and education requirements essential to support the AI workforce and the Total Force.

Strategic Goal 3:
AI Deployment at Scale

Objective 1 - Data Culture

- **Lead Department:** DC I
- **Timeframe:** End Date: NLT Apr 2026

- **Task: 3.1.1:** DC I, incorporate data-centricity into all levels of inspection programs to be inspected annually, and establish a baseline for the data culture to measure progress against. This includes, but is not limited to, the Commanding General's Inspection Program and other Service and Marine Expeditionary Force-level inspection programs.

- **Task: 3.1.2:** DC I, update Marine Corps Tactical Publication 3-30B Information Management to incorporate the changing dynamics of data-centricity and AI technologies on information management.

Objective 2 - Data Management

- **Lead Department:** DC I
- **Timeframe:** End Date: NLT Dec 2025

- **Task: 3.2.1:** DC I, in coordination with CD&I and Commander MCSC, establish a data architectural framework that informs the requirements development and procurement process for establishing an enterprise data solution that employs data standards, application programming interface- (API-) based services, and AI solutions.

Objective 3 - AI Infrastructure and Tools

- **Lead Department:** DC I
- **Timeframe:** End Date: NLT Dec 2026

- **Task: 3.3.1:** DC I, establish and coordinate an AI infrastructure OPT as a component of the AIWG to identify and accelerate immediate infrastructure requirements for cloud, on premises, and tactical applications. The OPT will also identify legacy systems for divestment. The output of this OPT will be presented to the AIWG for Service-level decision and will include recommendations on the following areas to enable machine learning operations:
  - Storage and compute
  - Development environment
  - Resource Management
  - Machine Learning platform

- **Task: 3.3.2:** DC I, develop a cost estimate over the future year defense plan (FYDP) for the implementation of this plan.

Objective 4 - Integration and Deployment

- **Lead Department:** DC CD&I
- **Timeframe:** End Date: NLT Sept 2026

- **Task: 3.4.1:** Commander MCSC, supported by DC I, and in coordination with Deputy Commandant for Installations and Logistics and CD&I, establish the requirement to retrofit lab environments at MCTSSA, the Marine Corps' Science and Technology Reinvention Laboratory (STRL), to allow for experimentation, testing, engineering, and integration of

Command, Control, Computing, Communications, Cyber, Intelligence, Surveillance, Reconnaissance and Targeting capabilities at all classification levels, up to the Top Secret/Sensitive Compartmented Information and Special Access Programs levels.

Objective 5 – Cybersecurity

- **Lead Department:** DC I
- **Timeframe:** End Date: NLT Sept 2027

- **Task: 3.5.1:** DC I, reform the Risk Management Framework to embrace automation and reduce administrative overhead. Ensure that reforms account for AI systems and support the timely approval of AI-related capabilities.

- **Task: 3.5.2:** DC I, provide data security posture management solution to enable data-centric security and Zero Trust.

- **Task: 3.5.3:** CG Marine Corps Forces Cyberspace Command (MARFORCYBER), enable and coordinate Defensive Cyberspace Operations **(**DCO) and cybersecurity functions to defend AI-enabled systems.

Strategic Goal 4:
AI Governance

Objective 1 - Responsible AI Governance

- **Lead Department:** DC I
- **Timeframe:** End Date: NLT Sept 2025

- **Task: 4.1.1:** DC I, through the AIWG, establish governance for safe, secure, ethical, and responsible AI for resource alignment across the Service. This governance will be lean yet effective, encouraging innovation while ensuring compliance. Incorporate applicable AI governance requirements into the Commanding General's Readiness Inspection for enforcement and oversight.

Objective 2 - Policies and Guidance

- **Lead Department:** DC I
- **Timeframe:** End Date: NLT Sept 2025

- **Task: 4.2.1:** DC I, conduct a policy analysis to identify gaps, inefficiencies, and where current policy does not align with strategic goals. Develop policies and guidance as determined from the analysis.

Strategic Goal 5:
Partnership and Collaboration

Objective 1 - Joint and Mission Partner Interoperability

- **Lead Department:** DC I
- **Timeframe:** End Date: NLT Sept 2026

- **Task: 5.1.1:** DC I, establish a plan for a 3-year USMC Center for Digital Transformation pilot.

Objective 2 - Academic Partnerships

- **Lead Department:** DC CD&I
- **Timeframe:** End Date: NLT Apr 2026

- **Task: 5.2.1:** DC CD&I, in conjunction with MCSC, DC M&RA, and CG TECOM, evaluate and seek to expand organizational relationships with university-affiliated research centers, academic institutions (e.g, Naval Postgraduate School), and federally funded research and development centers as it relates to AI problem sets.

- **Task: 5.2.2:** CG TECOM, in support of DC CD&I, evaluate adjacent service academia partnerships for expanded relationships.

Objective 3 - Industry Partnerships

- **Lead Department:** Commander MCSC
- **Timeframe:** End Date: NLT Dec 2025

- **Task: 5.3.1:** Commander MCSC, establish cooperative agreements and contracting vehicles for AI development and adoption.

- **Task: 5.3.2:** Commander MCSC, establish and coordinate regular industry-focused events for info sharing and capability demonstrations that contribute to awareness and adoption of relevant technologies.

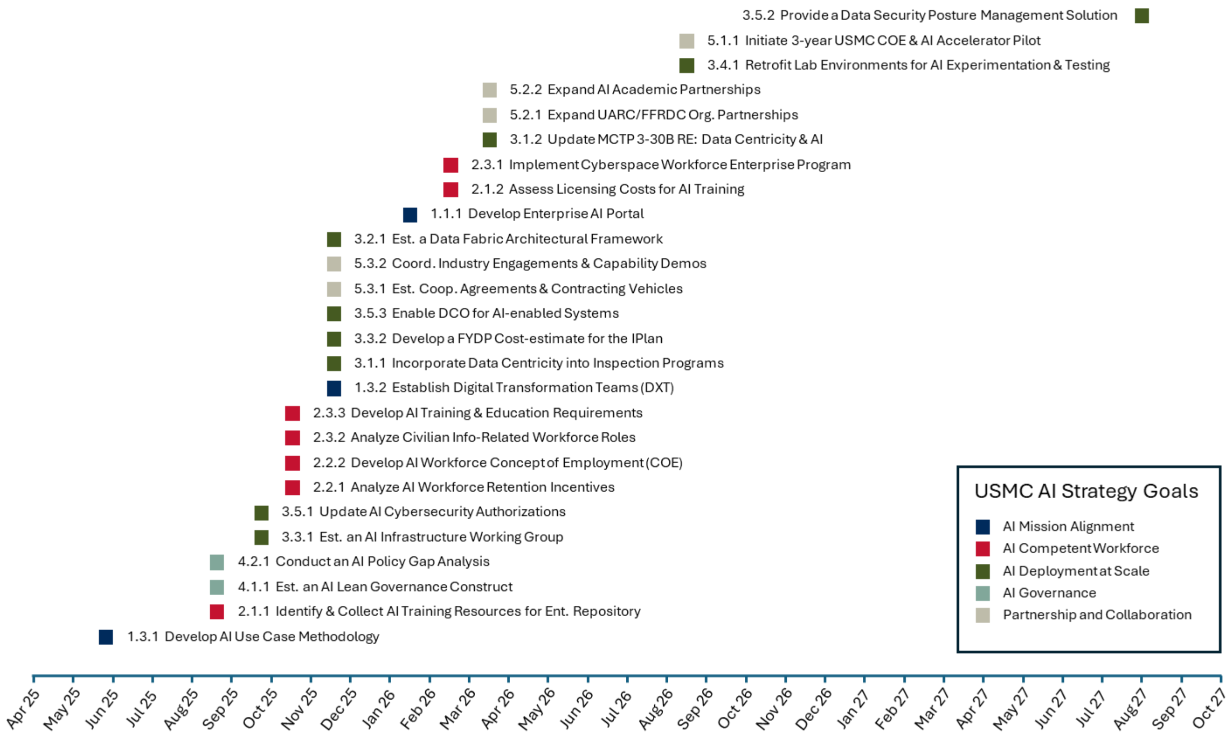


Figure 5. Implementation Plan Task Timeline

Conclusion

This AI IPlan provides a structured approach for integrating AI into Marine Corps operations through five primary goals: AI Mission Alignment, AI Competent Workforce, AI Deployment at Scale, AI Governance, and Partnerships and Collaboration. It outlines a Digital Transformation Pilot project as the leading edge of implementation, assesses the potential need for a Center for Digital Transformation, and underscores the importance of institutionalizing digital operations.

By aligning AI activities with mission requirements, advancing workforce development, modernizing infrastructure, establishing responsible governance, and strengthening partnerships, the Marine Corps positions itself to adapt to evolving technologies and maintain operational effectiveness. This plan facilitates the development of data and AI infrastructure and fosters the responsible use of AI to ensure an enduring information advantage. Future actions will focus on scaling key capabilities, formalizing governance structures, expanding AI-focused training, operationalizing data practices, and broadening collaborations for continued progress.

Through these deliberate steps, the Marine Corps ensures it remains prepared to meet emerging challenges and uphold its commitment to mission success.

Endnotes

[1] USMC Artificial Intelligence Strategy, Jul 2024
[2] 39th Commandant's Planning Guidance, Aug 2024
[3] Force Design 2030
[4] Department of Defense Data, Analytics, and Artificial Intelligence Adoption Strategy
[5] Executive Order on Removing Barriers to American Leadership in Artificial Intelligence
[6] Implementing Reasonable Artificial Intelligence in the Department of Defense
[7] U.S. Department of Defense Responsible Artificial Intelligence Strategy and Implementation Pathway, Jun 2022
[8] The Digitization Process: What Has it Led to, and What Can we Expect in the Future, Aslanvo H & Mirzagayeva S., 2022
[9] DC I Data Implementation Plan (DRAFT)
[10] USMC Zero Trust Implementation Plan, Jul 2024
[11] MCO 5231.4, Marine Crops Data and Artificial Intelligence
[12] Department of Defense Compliance Plan for Office of Management and Budget Memorandum M-24-10

Acronym List

Acronym	Explanation
AI	Artificial Intelligence
AI IPlan	Artificial Intelligence Implementation Plan
AIWG	Artificial Intelligence Working Group
DXT	Digital Transformation Teams
ATO	Authority to Operate
C5ISRT	Command, Control, Computing, Communications, Cyber, Intelligence, Surveillance, Reconnaissance and Targeting
DC	Deputy Commandant
DCIPS	Defense Civilian Intelligence Personnel Support
DEVSECOPS	Development Security Operations
DIWF	Defense Intelligence Workforce Framework
DoD	Department of Defense
DON	Department of the Navy
DOSC	Digital Operations Support Center
DOTMLPF-P	Doctrine, Organization, Training/Education, Materiel, Leadership, Personnel, Facilities and Policy Development
ETL	Extract, Transform, and Load
FAM	Functional Area Manager
FDM	Functional Data Manager
FDWG	Functional Data Working Group
FFRDC	Federally-funded Research and Development Centers
FYDP	Future Years Defense Plan
GRETR	Governable, Responsible, Equitable, Traceable, & Reliable
IAS	Intelligent Autonomous Systems
IATT	Interim Authority To Test
KPIs	Key Performance Indicators
LLM	Large Language Models
MCCDX	Marine Corps Center for Digital Transformation
MCIEE	Marine Corps Information Environment Enterprise
MCO	Marine Corps Order
MCSWF	Marine Corps Software Factory
ML	Machine Learning
MLOps	Machine Learning Operations
MOS	Military Occupational Specialty
NLP	Natural Language Processing
OCRs	Offices of Coordinating Responsibility
OPRs	Offices of Primary Responsibility
POM	Program Objective Memorandum
PORs	Programs of Records
RAI	Responsible Artificial Intelligence
RPA	Robotic Process Automation
RMF	Risk Management Framework
STRL	Science and Technology Reinvention Laboratory
SDO	Service Data Office
TEVV	Test, Evaluate, Validation, and Verification
UARC	University-affiliated Research Centers
VAULTIS	Visible, Accessible, Understandable, Linked, Trustworthy, Interoperable, and Secure

Definition of Terms

Term	Definition
Artificial Intelligence	The term "artificial intelligence" or "AI" has the meaning set forth in 15 U.S.C. 9401(3): a machine-based system that can, for a given set of human-defined objectives, make predictions, recommendations, or decisions influencing real or virtual environments. Artificial intelligence systems use machine- and human-based inputs to perceive real and virtual environments; abstract such perceptions into models through analysis in an automated manner; and use model inference to formulate options for information or action.
AI Model	A component of an information system that uses AI algorithms for statistics-based computations to conduct regression, clustering, prediction, classification, reinforcement learning and other techniques to produce outputs from a given set of inputs. This also includes generating synthetic content.
AI System	Any data system, software, hardware, application, tool, or utility that operates in whole or in part using AI.
AI Workforce	There are three primary groups critical to AI implementation: the Marines who utilize AI capabilities to enhance operational effectiveness; the AI workforce that builds, maintains, and refines advanced digital and AI solutions; and the leadership charged with making risk decisions on the use of AI.
Data Architecture	The pipes that deliver the fuel for consumption across the diverse, complex enterprise, and multi-cloud environment
Data Centricity	An architectural approach that results in a secure environment separating data from applications and making data available to a broad range of tools and analytics within and across security domains for enrichment and discovery. This environment embraces a more disciplined approach to intelligence integration by ensuring that data is sharable, discoverable, accessible, understandable, retrievable, and protected.
Data Culture	The collective behaviors and beliefs of people within an organization who value, practice, and encourage the use of data to improve mission and business outcomes. As a result, data centric policies, processes, standards, tools, and techniques are woven into organizational strategies, analysis, operations, and decision making.
Data Fabric	A design concept that serves as a federated and integrated layer (fabric) of data, and connecting processes for sharing information through interfaces and services to discover, understand, and exchange data with partners across all applications, domains, echelons, and security levels. Note: At a minimum, the implementation of the design concept must support cataloging, data event messaging, interface management, and access management capabilities.
Data Governance	A discipline comprised of responsibilities, roles, functions, and practices, supported by authorities, policies, and decisional processes (planning, setting policies, monitoring, conformance, and enforcement), which together administer data and information assets across an IC element to ensure that data is managed as a critical asset consistent with the organization's mission and business performance objectives

Data Leakage	Data leakage in machine learning occurs when a model uses information during training that wouldn't be available at the time of prediction. Leakage causes a predictive model to look accurate until deployed in its use case; then, it will yield inaccurate results, leading to poor decision-making and false insights.
Data Management	The development and execution of plans, policies, programs and practices (4Ps) that acquire, control, protect, and enhance the value of data assets throughout the lifecycle, led or performed by tradecraft professionals following established disciplines and functions
Data Pipeline	A set of tools and processes to automate or otherwise enable the movement, transformation, and optimization of data from a source to a destination.
Data Products	Data products are highly trusted, re-usable, and consumable data assets; they are curated collections of productized datasets and approved metadata and domain logic designed to solve domain-specific business outcomes.
Data Security	The ability to protect data resources from unauthorized discovery, access, use, modification, and/or destruction. Secure data sharing relies on several key functions: data identification, categorization, and labeling; entitlement management; and policy establishment. Note: Data Security is a component of Data Protection
Database	An organized collection of datasets generally stored and accessed from a computer system that allows the data to be easily searched, manipulated, and updated
Machine Learning	A set of techniques that can be used to train AI algorithms to improve performance at a task based on data.
Predictive Analytics	A form of advanced analytics that uses both new and historical data to determine patterns and predict future outcomes and trends.
Reinforcement Learning	A method of training algorithms to make suitable actions by maximizing rewarded behavior over the course of its actions. This type of learning can take place in simulated environments, such as game-playing, which reduces the need for real-world data
Responsible AI	A dynamic approach to the design, development, deployment, and use of AI capabilities that implements DoD Al Ethical Principles to advance the trustworthiness of Al capabilities. RAI emphasizes the necessity for technical maturity to build effective, resilient, robust, reliable, and explainable AI, while recognizing the value of multidisciplinary teams to advise on ethics, accountability, and risk.
Testbed	A facility or mechanism equipped for conducting rigorous, transparent, and replicable testing of tools and technologies, including AI and Privacy Enhancing Technologies (PETs), to help evaluate the functionality, usability, and performance of those tools or technologies.

Appendix A: Digital Transformation Pilot Project

The Digital Transformation Pilot project is designed to support commanders in identifying and delivering digital, data, and AI solutions to business and operational use cases. This pilot is key to transforming the Force into a data-centric organization to leverage advanced technologies. Digital Transformation Teams will be deployed as outlined below and incorporated into the Marine Corps governance structures to ensure sufficient support, oversight, and feedback is available. The composition of each team will vary based on the needs of each command.

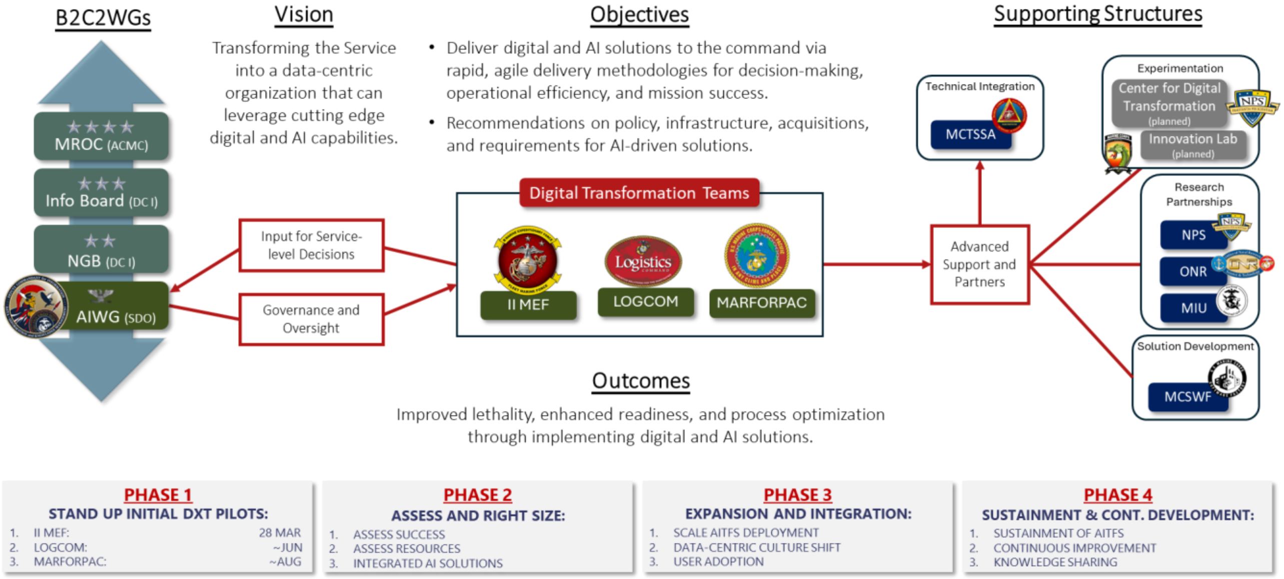
The integration of technology into core functions to achieve measurable gains often takes 3-5 years, or longer. This underscores the urgency for adoption of digital, data, and AI technologies now, while setting clear expectations for measurable results. As a cross-functional technology, AI introduces complexities that make success difficult to measure, requiring careful planning and monitoring to fully measure the impacts.

Objectives:

1. Deliver digital, data, and AI solutions to the command via rapid and agile delivery methodologies to enhance decision-making, operational efficiency, and mission success.
2. Provide input from across the Force on policy, resource, infrastructure, and acquisitions requirements to conduct agile delivery and ensure solutions are scalable, secure, and effective.

Governance and Reporting Structure:

- The Digital Transformation Teams will brief the AIWG on at least a quarterly basis.
- The Digital Transformation Teams mission and responsibilities include:
    - Provide the command with integrated digital capabilities that digitize and optimize processes, establish robust data pipelines, deliver advanced analytics, and implement AI-driven solutions to enhance operational effectiveness.
    - Advise the commander and staff on opportunities and risk with adopting solutions.
    - Provide a regular briefing and report to the AIWG on critical opportunities and challenges related to AI implementation.
- The AIWG will present artifacts to the Information Board for recommendations to the Marine Requirements Oversight Council on decisions impacting AI employment across the Service.


B2C2WGs
★★★★
MROC (ACMC)
★★★
Info Board (DC I)
★★
NGB (DC I)
AIWG (SDO)
Vision
Transforming the Service into a data-centric organization that can leverage cutting edge digital and AI capabilities.
Objectives
• Deliver digital and AI solutions to the command via rapid, agile delivery methodologies for decision-making, operational efficiency, and mission success.
• Recommendations on policy, infrastructure, acquisitions, and requirements for AI-driven solutions.
Input for Service-level Decisions
Governance and Oversight
Digital Transformation Teams
II MEF
LOGCOM
MARFORPAC
Supporting Structures
Technical Integration
MCTSSA
Advanced Support and Partners
Experimentation
Center for Digital Transformation (planned)
Innovation Lab (planned)
Research Partnerships
NPS
ONR
MIU
Solution Development
MCSWF
Outcomes
Improved lethality, enhanced readiness, and process optimization through implementing digital and AI solutions.

PHASE 1
STAND UP INITIAL DXT PILOTS:
1. II MEF: 28 MAR
2. LOGCOM: ~JUN
3. MARFORPAC: ~AUG

PHASE 2
ASSESS AND RIGHT SIZE:
1. ASSESS SUCCESS
2. ASSESS RESOURCES
3. INTEGRATED AI SOLUTIONS

PHASE 3
EXPANSION AND INTEGRATION:
1. SCALE AITFS DEPLOYMENT
2. DATA-CENTRIC CULTURE SHIFT
3. USER ADOPTION

PHASE 4
SUSTAINMENT & CONT. DEVELOPMENT:
1. SUSTAINMENT OF AITFS
2. CONTINUOUS IMPROVEMENT
3. KNOWLEDGE SHARING

Figure 6. USMC AI ecosystem and support to the Digital Transformation Teams.

Phase 1: Pilot Digital Transformation Team Deployment

Timeline: 6-12 months

- Deploy **three** Pilot Digital Transformation Teams within the following commands:
    - II Marine Expeditionary Force (MEF)
        - Sufficient structure exists and is being developed within II MEF to support the successful deployment of a Digital Transformation Team. This is an opportunity to contribute additional resources to support the effort initiated by II MEF.
    - Logistics Command (LogCom)
        - Sufficient structure exists and is being developed within LogCom to support the successful deployment of a Digital Transformation Team. This is an opportunity to contribute additional resources to support the effort initiated by LogCom.
    - Marine Corps Forces Pacific (MARFORPAC)
        - AI is and will continue to play a significant role in the pacific. MARFORPAC supports I and III MEF, making up most of the combat power in the Marine Corps. A Digital Transformation Team located at MARFORPAC is critical for integrating data and AI solutions in the Pacific.
- Focus Areas and Deliverables:
    - **Use Case Collection**: Collect, assess, and prioritize data and AI use cases.
    - **Data Product and AI Pipelines:** Develop data and AI pipelines and products that support scaling and transitioning of prototypes to production.
    - **Key Stakeholders**: Identify key stakeholders to ensure early integration.
    - **Prototyping**: Develop and prototype solutions based on identified use cases.
    - **Agile Methodology**: Assess the impacts and blockers to employ agile methodologies.

- Decision Point:
    - Evaluate the Digital Transformation Teams based on performance metrics and decide whether to continue with the pilot.
    - Evaluate emerging teams from commands not identified in this pilot for inclusion in the Digital Transformation Pilot.

Phase 2: Assess and Right Size

Timeline: 12-24 months

- Focus Areas and Deliverables:
    - **Performance Assessment Report**: Assess the successes, challenges, and overall performance of the Digital Transformation Teams.
    - **Revised Digital Transformation Team Structure**: Modify Digital Transformation Team composition, resourcing, and roles based on the assessment findings.
    - **Integrated Solutions**: Deploy and integrate solutions into existing systems and determine infrastructure needs for increased deployments.
    - **Use Case Enhancements**: Refine the collection of use cases and make improvements based on feedback and performance data.
    - **Agile Methodology**: Enhance agile practices to improve efficiency and adaptability.

- Decision Point:
    - Based on the success of the Digital Transformation Teams, decide whether to stand up additional Digital Transformation Teams.
    - Based on assessment report and readiness, decide whether to adjust Digital Transformation Team composition.

    - If significant challenges (e.g. infrastructure limitations, platform inadequacies, workforce skill gaps, etc) are reported that impact enterprise-wide deployment, decide whether to invest in necessary enhancements to address the identified capability gaps.

Phase 3: Expansion and Integration

Timeline: 24-36 months

- Focus Areas and Deliverables:
    - **Scaled Digital Transformation Team Deployment:** Expand Digital Transformation Teams to additional commands across the Service.
    - **Data and AI Solutions Portfolio:** Delivering data and AI solutions, providing the AIWG with insights on broader capability gaps.
    - **Data Culture Transformation:** Support data culture shift via inspectable programs to enhance a positive data culture.
    - **Advanced Data and AI Governance Policies:** Develop and enforce comprehensive data and AI governance policies to support the expanded data and AI integrations.
    - **User Adoption:** Ensure user training and support for deployed AI systems.

- Decision Point:
    - Decide whether to transition the Digital Transformation Pilot to sustained structure across the Service, modify the concept and extend the pilot, or terminate the pilot program.

Phase 4: Sustainment and Continuous Development

Timeline: Ongoing

- **Sustainment of Digital Transformation Teams:** Persistent Digital Transformation Teams embedded across major commands.
- **Continuous Improvement**: Continually refine systems, data and AI pipelines, and data products based on performance metrics and user feedback.
- **Knowledge Sharing Platforms**: Provide best practices, lessons learned, and innovations across the AI community via a knowledge sharing platform.
- **Feedback Loop**: Digital Transformation Teams continuously assess emerging threats, technologies, and operational needs to refine data and AI solutions.

Digital Transformation Teams Composition (Generic Example)**:**

Core Squad (6-8 Personnel):

- (1) Team Lead (O-4/O-5): Directs delivery and integration into mission planning and operations.
- (1) Product Manager: Prioritizes development sprints based on mission requirements.
- (1) Data/AI Engineer: Design, develop, and maintain data integration, pipelines, products, infrastructure, and deployment.
- (1) Data Scientist: Responsible for modeling, analytics, and experimentation.
- (1) User Interface/User Experience Engineer: Front end requirements for product development and deployment.
- (1-3) Operational SMEs: Provide cross-functional SMEs to guide product development.

Technical Support Structure:

- MCTSSA will act as the primary technical support to the Digital Transformation Teams.
- MCTSSA's Warfighter Support Division provides a 24/7 Global Support Branch that is tightly integrated with their Digital Solutions Branch.
- This capability provides the Digital Transformation Teams the ability to augment their team with mission-funded software developers, providing additional depth of bench for exquisite AI capabilities.

- MCTSSA’s STRL designation allows the capability to surge additional contractors on short timelines to ensure mission success.

Metrics for Success:
The pilot will first target initial operating capability while working toward achieving full operating capability. Metrics for success will be updated as applicable.

- Blocker Identification
    - Identification of significant challenges impeding digital transformation, adoption, and integration.
- Backlog Growth and Completion
    - The ratio of completed use cases or tasks to newly added ones.
- User Adoption Rates
    - Number of intended users that are actively using delivered solutions, tolls, or processes and how often.
- Reduction in Manual Work and Reduction in Process Delays
    - The percentage of tasks automated or manual steps eliminated in the workflows.
    - % of new data integrations achieved.
- Time-to-Value
    - Average time from project start to delivery of a functional prototype or minimum viable product.
- Infrastructure Growth
    - Improvement to development environments, data pipelines, and MLOps solutions.
- Training and Education
    - Number of informal and formal courses on data, AI, and related topics offered and completed by Marines within the command.

Key Outputs to AIWG:

- Quarterly AI Capability Reports:
    - Detailing the AI capabilities delivered, operational performance, and identified opportunities and challenges.
    - Demonstrating cost savings, readiness improvements, and warfighting enhancements from AI initiatives.
- Quarterly Strategic Recommendations:
    - Highlighting infrastructure, policy, and acquisition changes required to scale AI capabilities across the force and the ability or limitations with applying agile methods.

Appendix B: Resourcing Framework

AI has become ubiquitous within DoD and US forces are employing AI-based capabilities as part of daily activities. AI is defined by the Department of Defense (DoD) as "the ability of machines to perform tasks that normally require human intelligence."[4] Planning and programming for AI technology will be challenging because AI cannot be separated from its software or machine hosts. Therefore, planning and programming for AI will focus on the end state e.g. AI enhanced software solutions and machines. When applicable, AI enhanced Software and Machine solutions will be discretely identified within the planning, programming, budgeting and execution processes.

Each Marine Corps AI enhanced system or program shall record all costs within the DON Program Budget Information System Information Technology. All resources shall be reported regardless of appropriation (Research, Development, Training & Education, Procurement, Military Construction, or Operation and Maintenance). At a minimum resourcing will be identified by Program Element, Budget Line Item, Project Code, Treasury Code, and Budget Activity Code.

AI resourcing costs shall be classified by three categories: AI Development, AI Integration and Application, and AI Support. The descriptions below characterize the types of activities that deliver AI capabilities to warfighters and across the enterprise:

- Development: AI development activities build and mature AI models, algorithms, and concepts that result in a capability that can be used in a system. This includes research, development, training, testing, and evaluation of AI technologies.

- Integration and Application: AI integration and application activities use AI to enable or aid analysis, automation, communication, maneuvering, monitoring, sensing, and other military activities. AI integration and application may occur in new or existing platforms and only comprise a portion of a larger platform or program, which may or may not be critically dependent upon its incorporation.

- Support: AI support activities promote the development, deployment, and use of AI to occur faster, at greater scale, and more responsibly. AI support may incorporate technologies such as data pipeline engineering that provides guardrails either using cloud computing or on premise for AI developers and users. Workforce training and collecting or buying data for an AI application also fall in this category.

Consumers shall identify the function or role the AI is performing. The four core functions are as follows:

Mission. Identify how the AI is supporting the greater mission e.g. enterprise, exploratory, unique or workforce.

Planning Horizon. Identify the planning horizon in which the AI System Program contributes or will contribute to operational capabilities or bridge, which fills gap between current and future capabilities

Use Case. Identifying the use case for the AI provides an understanding of the specific ways that AI is being employed and aids in the identification of requirements for common services or infrastructure. This information enables reporting on use cases, in compliance with inter-agency regulations and the DoD Responsible AI Strategy & Implementation Pathway. Use cases should be reported at the appropriate level of classification. Unclassified examples include generation of language for press releases; object detection; optimization of schedules; and predictive maintenance:

National Security System. Identify the AI that is leveraged or used that (I) involves intelligence activities; (II) involves cryptologic activities related to national security; (III) involves command and control of military forces; (IV) involves equipment that is an integral part of a weapon or weapons system; or (V) subject to subparagraph (B), is critical to the direct fulfillment of military or intelligence missions; or (ii) is protected at all times by procedures established for information that have been specifically authorized under criteria established by an Executive order or an Act of Congress to be kept classified in the interest of national defense or foreign policy.

Existing Marine Corps programs and initiatives will continue to incorporate and or adopt AI. Regardless of organization, coordination across these programs and initiatives is imperative to ensure appropriate resource prioritization, facilitate service needs, and ensure a uniform approach to the implementation of the USMC AI Strategy.

Appendix C: Requirements Alignment

Following the release of the USMC AI Strategy, an assessment was conducted to determine alignment of existing requirements to the goals and objectives outlined. Where a requirement is not identified or does not fully meet the end state of the goals and objectives outlined in the USMC AI Strategy, a gap exists that will be included in the annual gaps list to be developed into a subsequent requirement.

The following documents provide established and approved requirements that direct support pursuit of materiel and non-materiel solutions. This is not an initial assessment and may not be comprehensive covering all applicable requirements documents.

Goal	**Requirements Document**
Goal 1: AI Mission Alignment	- DoD Transition Tracking Action Group Charter – 13 Mar 2024
Goal 2: AI Competent Workforce	- OSD Memo for Department-wide Initiative to Assign and Code Work Roles Related to Data, Artificial Intelligence, and Software Engineering (“Digital Workforce”) – 5 Jan 2024
Goal 3: Deploy AI at Scale	- DODI 8320.02, Sharing Data, Information, and Technology (IT) Services in the Department of Defense – 5 Aug 2013 - DODI 8500.01, Cybersecurity, 14 Mar 2014, Change 1 – 7 Oct 2019 - DoD Zero Trust Reference Architecture Version 2.0 – 4 Jul 2022 - DoD Zero Trust Strategy – 21 Oct 2022 - DoD Cybersecurity Reference Architecture, Version 5.0 – 20 Feb 2023 - USMC AI Capabilities Based Assessment – 7 Jul 2023 - DON Strategic Intent to Implement Zero Trust – 8 Aug 2023 - USMC Zero Trust Implementation Plan, Version 1 – 9 Jul 2024
Goal 4: AI Governance	- DoD Responsible AI Strategy and Implementation (S&I) Pathway – 22 Jun 2022 - DoD Data, Analytics, and AI Adoption Strategy – 27 June 2023
Goal 5: Partners and Collaboration	- DoD AI Strategy – 12 Feb 2018 - DepSecDef AI and Data Acceleration Initiative – 1 Feb 2021 - National Defense Strategy (NDS) – 27 Oct 2022 - DoD Data, Analytics, and AI Adoption Strategy – 24 Jan 2023

Appendix D: Measurement and Assessment

This appendix is intended as a starting point for OPRs to build key performance indicators (KPIs) for each task. OPRs are encouraged to break down tasks further into sub-tasks with metrics where applicable. The placeholder values in the Target Value column will be updated by OPRs prior to the first quarterly update.

Task	KPIs	Metrics	Target Value	Measurement Method
Task: 1.1.1: DC I, in coordination with Commander MCSC and PEO-DES, facilitate the development of a centralized enterprise portal on all relevant network enclaves to communicate, at a minimum, the following: Training and education resources, available AI capabilities, AI policies and guidance.	Enterprise Portal Document Count and Currency	Percent of necessary resources and percent of capabilities, policies and guidance updated annually.	100% resources, capabilities, policies and guidance reviewed and updated.	Count and last review/update date stamps.
Task: 1.2.1: DC CD&I, in coordination with DC I, continuously review urgent need statements across the Service and decompose them into capability requirements, transitioning them into requirement documents. Update key performance parameters, objective values, and threshold values based on the projected state-of-the-art capabilities, and develop standard requirements lexicon for use across programs and warfighting functions as applicable.	Number of use cases and projects selected for implementation with supporting requirements updated across PoRs	Percent of use cases fully analyzed and integrated into PoRs.	75% of use cases transitioned into requirements with updated parameters.	Track use case status from collection to requirements generation, noting analysis, decomposition, and updates.
Task: 1.2.2: DC CD&I, in coordination with acquisition communities, develop transition plans for initiatives that demonstrate high return on investment. Transition plans will apply the DOTMLPF for adoption of a capability over a pre-defined timeline	High-TRL Pilot to PoR Transition Rate	Percent of high-TRL pilots integrated into PoRs during evaluation.	X% of high-TRL pilots transitioned into PoRs.	Monitor and record transitions from pilot to PoR integration.
Task: 1.3.1: DC I, in coordination with DC CD&I, develop a use case methodology that captures, assesses, and prioritizes concepts for the application of AI from across the warfighting functions, and at all echelons, to implement targeted actions. Through the collection of use cases, identify major roadblocks in policy, workforce, and infrastructure that have a large impact on innovation and acceleration of AI implementation to mitigate through change.	AI Use Case Development and Maturity Index	Number of AI use cases captured and percentage reaching maturity.	Increase use case capture quarterly, X% mature.	Observe use case tally and maturity stage advancement.
Task: 1.3.2: DC I, oversee the establishment of the Digital Transformation Pilot as described in Appendix A to support commanders with implementing and incorporating digitization, data, analytics, and AI across their commands. Incorporate the Digital Transformation Teams into data and AI governance for resource alignment, oversight, and Service-level decisions.	Digital Transformation Pilot Establishment Progress	Percent of G/O commands with operational Digital Transformation Teams.	X% Digital Transformation Teams established.	Document establishment and operational status of Digital Transformation Teams.

Task	KPIs	Metrics	Target Value	Measurement Method
<u>Task: 2.1.1</u>: CG TECOM, identify available learning tools, resources, and current use-cases across the DoD and industry and centralize these resources into a repository for proactive learning, ensuring commanders and leaders are empowered to promote and authorize AI training.	AI E-Learning Participation Rate	Total number of Marines completing AI e-learning training.	X Marines trained.	Monitor enrollments, completions, and feedback in e-learning system.
<u>Task: 2.1.2</u>: CG TECOM, identify costs and requirements for licensing external training resources outside of the USMC, while aligning with FMF capabilities and existing PoRs to enable shared funding and rapid acquisition in order to determine long term viability and funding.	AI Training Proficiency and Resource Alignment	AI task proficiency levels per T&R standards and alignment of training resources with FMF needs.	Attain average proficiency score X and Y external training resource licenses.	Evaluate post-training AI proficiency and monitor training resource agreements.
<u>Task: 2.2.1</u>: DC M&RA analyze career retention compensation opportunities, to include, at a minimum, monetary, billet preference, established career progression opportunities that support the development and retention of the AI workforce.	AI Workforce Incentive Alignment Index	Number of AI-related positions created, manned, and retained.	Launch X AI-related positions career incentives.	Monitor development, sanction, and activation of incentives in the career system.
<u>Task: 2.2.2</u>: DC I, develop and submit the concept of prospectus that supports the Digital Operations Concept for consideration via the DOTMLPF process.	Operational Streamlining Effectiveness	Number of operational areas for tech streamlining and percent of transitions to CDD/Capability Needs Statements.	Pinpoint X areas and convert Y% into CDDs/CNSs.	Record workflow assessments, streamlining opportunities, and formal document transitions.
<u>Task: 2.3.1</u>: DC I, implement and lead the Marine Corps Cyberspace Workforce Enterprise Program to expand development resources, such as the Information Development Institute, and bolster support for data analytics.	Cyberspace Workforce Qualification Achievement Rate	Percent of personnel meeting DoD 8140/8570 standards.	Qualify X% of targeted workforce.	Use TFSMS or MCTIMS to monitor qualifications and resources.
<u>Task: 2.3.2</u>: DC M&RA, supported by DC I, ensure the information-related civilian workforce is included in AI workforce modernization. Analyze how to maximize return on investment in the civilian information-related workforce segment; methods to standardize the prediction of future civilian workforce needs; how to improve position descriptions; how to speed hiring; and how to make civilian workforce data more accessible for talent management initiatives.	Civilian Workforce Talent Management Optimization Index	Enhancements in time-to-hire, workforce prediction accuracy, and data access.	Cut time-to-hire by X%, boost prediction accuracy by Y%, enhance data access by Z%.	Compare past and present data to measure hiring efficiency, forecasting precision, and data system upgrades.
<u>Task: 2.3.3</u>: CG TECOM, develop and institutionalize the training and education requirements essential to support the AI workforce and the Total Force.	Training and Education Requirements Development Completion	Rate of T&E solutions developed and published for echelons and billets.	Complete T&E solutions for X% of echelons and billets.	Monitor and document T&E development from analysis to publication against capability requirements.

Task	KPIs	Metrics	Target Value	Measurement Method
Task: 3.1.1: DC I, incorporate data centricity into all levels of inspection programs to be inspected annually, and establish a baseline for the data culture to measure progress against. This includes, but is not limited to, the Commanding General's Inspection Program, and other Service and Marine Expeditionary Force-level inspection programs.	Data Centricity Inspection Integration and Compliance Rate	Data-centricity questions included in CGRI, CGRIs conducted, and MCO 5231.4 compliance.	Add X data-centricity questions to CGRI, perform Y CGRIs with these questions, and reach Z% compliance.	Monitor data-centricity question integration, count CGRIs conducted, and assess compliance rates.
Task: 3.1.2: DC I, update Marine Corps Tactical Publication 3-30B Information Management to incorporate the changing dynamics of data-centricity and AI technologies on information management.	Tactical Publication 3-30B updated and published	Percent completion based on update timeline.	100% completion of the publication revisions.	Document progress tracking.
Task: 3.2.1: DC I, in coordination with CD&I and Commander MCSC, establish a data architectural framework that informs the requirements development and procurement process for establishing an enterprise data solution that employs data standards, API-based services, and AI solutions.	Data Architecture Framework Establishment.	Percent completion of the data architecture framework.	100% completion of the data plan, with at least three integration milestones met, demonstrating functional services and support	Progress reviews at defined milestones against the established timeline and deliverables, concluding with a formal validation by DC I, CD&I, and MCSC by NLT June 2025.
Task: 3.3.1: DC I, establish and coordinate an AI infrastructure OPT as a component of the AIWG to identify and accelerate immediate infrastructure requirements for cloud, on premises, and tactical applications. The OPT will also identify legacy systems for divestment. The output of this OPT will be presented to the AIWG for Service-level decision and will include recommendations on the following areas to enable machine learning operations: - Storage and compute - Development environment - Resource Management - Machine Learning platform	AI Infrastructure Working Group Deliverables	Identification of AI infrastructure requirements needed across different environments.	Present full AI infrastructure requirement list to SDO.	Track AI infrastructure working group sessions, requirements gathered, and preparation progress for the SDO presentation.
	Legacy Systems Identification for Divestment	Legacy systems flagged for divestment by AI Infrastructure WG.	Pinpoint X legacy systems for divestment.	Log and monitor the legacy system identification and evaluation process.
Task 3.3.2: DC I, develop a cost estimate over the FYDP for the implementation of this plan.	Implementation Plan Cost Estimate.	Completion of an approved cost estimate.	Complete and approved.	DC I will develop a cost estimate over the FYDP for the implementation of this plan.

Task	KPIs	Metrics	Target Value	Measurement Method
Task: 3.4.1: Commander MCSC, supported by DC I, and in coordination with Deputy Commandant for Installations and Logistics (DC I&L) and CD&I, establish the requirement to retrofit lab environments at MCTSSA, the Marine Corps' Science and Technology Reinvention Laboratory (STRL), to allow for experimentation, testing, engineering, and integration of Command, Control, Computing, Communications, Cyber, Intelligence, Surveillance, Reconnaissance and Targeting capabilities at all classification levels, up to the Top Secret/Sensitive Compartmented Information and Special Access Programs levels.	MCTSSA STRL Lab Retrofitting Requirements Articulation	Development and approval status of requirements for retrofitting MCTSSA STRL labs for DEVSECOPS support.	Complete and sanction requirements document(s).	Monitor stages from drafting to approval of the retrofitting requirements document(s).
Task: 3.5.1: DC I, reform the Risk Management Framework to embrace automation and reduce administrative overhead. Ensure that reforms account for AI systems and support the timely approval of AI-related capabilities.	AI Authorization Guidance Integration	Percent of Marine Corps Authorization documents revised to contain AI guidance.	100% of pertinent documents include AI authorization guidance.	Monitor updates and validate AI guidance inclusion in authorization documents, comparing against the total needing revisions.
Task: 3.5.2: DC I, provide data security Posture management solution to enable data-centric security and Zero Trust.	Deployment and Effectiveness of Data Security Posture Management Solution	Extent of Data Security Posture Management solution's implementation and its operational effectiveness.	Attain complete deployment and operational effectiveness.	Follow deployment stages, verify integration, and evaluate effectiveness via security posture evaluations.
Task: 3.5.3: CG MARFORCYBER, enable and coordinate DCO and cybersecurity functions to defend AI-enabled systems.	Resolution and Mitigation of Incidents on AI-enabled Systems	Count of security incidents resolved or mitigated on AI systems.	Resolve or mitigate X incidents with Y% severity reduction.	Record incident responses and evaluate effectiveness and severity reduction.
Task: 4.1.1: DC I, through the AIWG, establish governance for safe, secure, ethical, and responsible AI for resource alignment across the Service. This governance will be lean yet effective, encouraging innovation while ensuring compliance. Incorporate applicable AI governance requirements into the CGRI for enforcement and oversight.	AI Governance Structure Implementation	Percent of AI governance frameworks successfully established and functional.	Fully establish and make operational all planned AI governance structures.	Monitor the setup and activation of governance systems, confirming their operational status and evaluating their role in AI stewardship.
	AI Governance Integration in CGRI	Percent of AI governance requirements that are fully integrated into the Commanding General's Readiness Inspection (CGRI).	Achieve 100% integration of AI governance requirements into the CGRI.	Monitor the revision process of the CGRI to include AI governance requirements and evaluate the completeness of their integration into the inspection protocol.

Task	KPIs	Metrics	Target Value	Measurement Method
Task: 4.2.1: DC I, conduct a policy analysis to identify gaps, inefficiencies, and where current policy does not align with strategic goals. Develop policies and guidance as determined from the analysis.	Identification of Policy Gaps and Inefficiencies	The number of policy gaps closed	Resolve X number of policy gaps.	Document and quantify the findings from the policy analysis, emphasizing the gaps and areas of inefficiency that require attention to align with AI strategic goals.
	Development and Approval of New Policies and Guidelines	Number of new policies and guidelines developed and formally approved that address the identified gaps and inefficiencies.	Develop and obtain formal approval for X new policies and guidelines.	Track the progression from draft to approval of new policies and guidelines. Documentation includes a verification of how each policy/guideline addresses the previously identified gaps and inefficiencies, ensuring alignment with strategic AI goals.
Task: 5.1.1: DC I, establish a plan for a 3-year USMC Center for Digital Transformation pilot.	Pilot plan is submitted to the DOTMLPF Working Group (DWG) for pilot designation.	Completion of action items for DWG submission.	100% of actions items complete and submitted to the DWG.	Track the progress of each action item, DWG submission, outcomes, and proof of concept opportunities.
Task: 5.2.1: DC CD&I, in conjunction with Commander MCSC, DC M&RA, CG MCWL and CG TECOM, evaluate and seek to expand organizational relationships with university-affiliated research centers and federally-funded research and development centers as it relates to AI problem sets.	UARC/FFRDC Partnership Development and Solution Transition	Percentage of AI problem sets with capability solutions pursued in partnership with UARCs/FFRDCs. Number of capability solutions from UARCs/FFRDCs transitioned to POR.	Partner with UARCs/FFRDCs for capability solutions on X% of AI problem sets by TBD. Transition X capability solutions from UARCs/FFRDCs to POR.	Percentage of AI problem sets being addressed in collaboration with UARCs/FFRDCs. The number of capability solutions transitioned from UARCs/FFRDCs collaborations to POR status.
Task: 5.2.2: CG TECOM, in support of DC CD&I, evaluate adjacent service academia partnerships for expanded relationships.	Joint Service Academic Engagement and Project Integration	Number of USMC students trained at joint service academia institutions and USMC projects that involve academia collaboration.	Reach a combined total of X instances of academic engagement (training and project collaboration).	Aggregate and assess the number of USMC students trained and the number of projects involving academia to measure the level of engagement and collaboration.
Task: 5.3.1: Commander MCSC, establish cooperative agreements and contracting vehicles for AI development and adoption.	Information Consolidation Efficiency	The magnitude and frequency of participation from stakeholders and industry.	Successfully establish and operationalize the consolidated information system.	Verify the creation and functionality of the information consolidation system, ensuring it effectively combines bottom-up and top-down information within the set timeframe.
Task: 5.3.2: Commander MCSC, establish and coordinate regular industry-focused events for info sharing and capability demonstrations that contribute to awareness and adoption of relevant technologies.	Industry Partnership and Technology Awareness	The magnitude and frequency of participation from stakeholders and industry.	Achieve X technology transfers to emerging and established POR.	Count and document the instances of technology transfer from industry to POR, confirming the use of CRADAs, PPAs, and evaluating the impact on POR modernization.

Appendix E: Change Management

The successful implementation of enterprise AI solutions will introduce transformative changes across the Service. These changes extend beyond technology deployment and require the integration of new behaviors, skills, and mindsets at all levels. This change management plan provides a structured approach to address human and organizational aspects of the transition. It outlines the frameworks, roles, responsibilities, communication strategies, training initiatives, resistance management techniques, and evaluation measures essential to ensuring Marines are fully supported and equipped to adopt and sustain AI-enabled capabilities. This is a Service-wide responsibility to ensure change is managed as AI systems are adopted. The aim is to foster a smooth transition that preserves readiness, maintains trust, and enhances operational effectiveness.

1. Guiding Principles and Framework

The following principles underpin the change management efforts and guide decision-making throughout the transition:

1. **Marines First**: Marines are central to design, development, and deployment efforts. Their feedback and insights inform solutions to meet operational needs.
2. **Leadership Commitment**: Leaders at all levels champion the change, model desired behaviors, and cultivate a positive command climate to inspire trust and engagement.
3. **Training and Support**: Adequate training, coaching, and resources ensure Marines confidently adopt new technologies, enhance their skills, and apply AI capabilities effectively.
4. **Proactive Resistance Management**: Leaders are equipped with tools and strategies to identify, understand, and mitigate resistance to change, leveraging command climate to encourage buy-in.
5. **Building Trust and Confidence**: Emphasize that AI is a force multiplier, designed to augment—rather than replace—Marines' warfighting capabilities.
6. **Consistent, Clear Messaging**: Reinforce the purpose, benefits, and long-term vision of AI through transparent, frequent communication that aligns with Marine Corps values.
7. **Cross-Organizational Collaboration**: Foster alignment and coordination among various units, functional areas, and support organizations to address interdependencies and authorities.
8. **Expectation Management**: Acknowledge that realizing AI's full impact is a long-term endeavor, influenced by evolving technologies, operational rhythms, and lessons learned.
9. **Continuous Engagement**: Maintain open communication channels, solicit feedback, and adapt strategies as lessons are learned, ensuring Marines remain engaged, informed, and motivated.

2. Stakeholder Engagement and Analysis

- **Identification**: Recognize key stakeholder groups, including leadership, end-users, support personnel, technology partners, and external allies.
- **Prioritization**: Assess stakeholder interest and potential impact to tailor engagement approaches.
- **Ongoing Involvement**: Regularly revisit stakeholder assessments as the implementation evolves, ensuring that communication and engagement remain targeted and relevant.

3. Communication and Messaging Strategy

- Increase awareness of AI capabilities, goals, and expected outcomes.
- Clarify roles, responsibilities, and benefits to individuals and units.
- Reinforce messages that align with Marine Corps values and mission readiness.

4. Training and Development

- Skill Development: Deliver hands-on training, simulations, and workshops tailored to Marines' operational contexts and proficiency levels.
- Sustainment: Provide ongoing refresher courses, micro-learning modules, and readily accessible support materials to reinforce new competencies over time.

5. Resistance Management and Cultural Adaptation

- Early Engagement: Anticipate common concerns and address them proactively through transparent communication and involvement in solution design.
- Leadership Advocacy: Equip leaders with frameworks and talking points to listen empathetically and guide Marines through the transition.
- Feedback Loops: Encourage open dialogue, promptly address concerns, and leverage success stories to illustrate tangible benefits and shift mindsets.

6. Monitoring, Evaluation, and Continuous Improvement

- Measure user adoption rates, utilization metrics, and performance improvements against established baselines.
- Assess training effectiveness, communication reach, and stakeholder satisfaction through surveys, feedback sessions, and after-action reviews.

By adhering to these principles and structures, the Marine Corps can navigate the complexities of AI adoption, ensuring that Marines remain at the center of decision-making, training, and support. This plan will help create a cultural and organizational environment where AI-enabled capabilities enhance mission effectiveness.

Appendix F: AI Risk Management

Risk management is an essential component for the safe, secure, and trustworthy development and deployment of AI. To ensure alignment with federal AI requirements and the Department of Defense directives, this appendix provides an approach to control selection and specification considering effectiveness, efficiency, and constraints with developing and deploying AI systems within applicable laws, directives, Executive Orders, policies, standards, or regulations.[13] This appendix will aide in ensuring that AI solutions are effective, efficient, and within the bounds of ethical and regulatory standards.[14]

The Executive Office of the President released the Office of Management and Budget (OMB) M-24-10[12] establishing guidance on the governance and risk management of AI for federal agencies. The OMB guidance requires agencies to appoint Chief AI Officers (CAIOs)[12] and follow minimum risk management practices when using safety impacting AI. The National Security Memorandum on AI echoes this to include specific governance and risk management requirements for high impact AI. In pursuant of these goals, the Department's Chief Digital and Artificial Intelligence Office (CDAO) has provided oversight and guidance with the Memorandum on Implementation Guidance for Federal AI Requirements, including outlining "Prohibited AI Use Cases" and a "Covered AI Use Case."[15]

Prohibited AI Use Cases

In addition to refraining from using AI in any manner that violates applicable legal or treaty obligations, the OMB Guidance and NSM prohibits the Department from using AI in any use cases that pose unacceptable levels of risk. Accordingly, the Department shall not use AI with the intent or purpose to:

1. Inform and execute decisions by the President to initiate or terminate nuclear weapons employment without a human "in the loop" for all critical actions.
2. Profile, target, or track activities of individuals based on the exercise of rights protected under the Constitution and applicable U.S. domestic law, including freedom of expression, association, and assembly rights.
3. Unlawfully suppress or burden criticism, dissent, or the free expression of ideas or political opinions; unlawfully suppress or restrict a right to legal counsel; or unlawfully disadvantage an individual based on their race, color, religion, sex, or national origin.
4. Fully automate the determination about whether an individual is permitted immigration, refuge, or asylum, or other entry in the United States.
5. Detect, measure, or infer an individual's emotional state from data acquired about that person, based solely on AI outputs and without appropriate human oversight, except for a lawful and justified reason, such as for the purposes of supporting the health of consenting U.S. Government personnel.
6. Produce or disseminate reports or intelligence analysis based solely on AI outputs without sufficient warnings that the intelligence is based solely on AI outputs, leadership approvals, and interagency notification of such AI use.

Covered AI Use Cases (Safety- and Rights-Impacting and High-Impact AI)

Covered AI is when AI serves as the principal basis for a corresponding decision or action that could impact national security, international norms, human rights, democratic values, or civil liberties in the event of an AI failure; to include rights or safety impacting.

The term "rights-impacting AI" refers to AI whose output serves as a principal basis for a decision or action concerning a specific individual or entity that has a legal, material, binding, or similarly significant affect on that individual's or entity's:

1. Civil rights, civil liberties, or privacy, including but not limited to freedom of speech, voting, human autonomy, and protections from discrimination, excessive punishment, and unlawful surveillance;
2. Equal opportunities, including equitable access to education, housing, insurance, credit, employment, and other programs where civil rights and equal opportunity protections apply; or
3. Access to or the ability to apply for critical government resources or services, including healthcare, financial services, public housing, social services, transportation, and essential goods and services.

The term "safety-impacting AI" refers to AI whose output produces an action or serves as a principal basis for a decision that has the potential to significantly impact the safety of:

1. Human life or well-being, including loss of life, serious injury, bodily harm, biological or chemical harms, occupational hazards, harassment or abuse, or mental health, including both individual and community aspects of these harms;
2. Climate or environment, including irreversible or significant environmental damage;
3. Critical infrastructure, including the critical infrastructure sectors defined in Presidential Policy Directive 21 or any successor directive and the infrastructure for voting and protecting the integrity of elections; or,
4. Strategic assets or resources, including high-value property and information marked as sensitive or classified by the Federal Government.

The National Institute of Standards and Technology (NIST) has developed an AI risk management framework NIST AI 600-1 to "improve the ability of organizations to incorporate trustworthiness considerations into the design, development, use, and evaluation of AI products, services, and systems." [13]

[13] NIST AI 600-1: AI Risk Management Framework
[14] 2020 DoD AI Ethical Principles
[15] Implementation Guidance for Federal Artificial Intelligence Risk Management Requirements

Appendix G: AI IPlan Threat Assessment

Introduction

This Appendix establishes key principles and methods to identify and assess the threats that adversaries may pose to Marine Corps artificial intelligence (AI) and Intelligence Robotics and Autonomous Systems (IRAS), as well as their operational employment. While offering extensive operational benefits, implementation of AI also introduces new vulnerabilities and risks. The Marine Corps should anticipate that adversaries may attempt to create and exploit vulnerabilities throughout the development and deployment lifecycle of Marine Corps AI capabilities. Examples include adversary actions to disrupt, degrade, deny, deceive, or defeat our AI systems. Adversaries may take these actions to seek one or more outcomes including: to exploit our reliance on these systems, to undermine our trust in them, or to gain a relative advantage in the application of their own AI capabilities. The Artificial Intelligence Risk Management Framework (AI RMF1.0)[16] published by the National Institute of Standards and Technologies is primarily focused on assessing and mitigating the risks to individuals, organizations, and society that can be posed by a given AI system. In contrast, this Appendix considers the threats posed by an adversary to our use of the AI system. By focusing on the nature and effects of threats, rather than specific adversaries or technologies, this Appendix provides an initial framework for more specific threat assessments. This framework is intended to be flexible and remain broadly relevant as AI technologies and adversaries continue to evolve and advance.

The imperative to understand and counter the adversary threat to Marine Corps AI systems was clearly articulated in a 2020 report which stated,

> "*Fielding AI systems before the competitors may not matter if DOD systems are brittle and break in an operational environment, are easily manipulated, or operators consequently lose faith in them. Military operations present a challenging environment. The Defense Department needs ML/DL systems that are robust and secure. They need to be able to function in a range of environmental conditions, against adversaries who are adaptive and clever, and in a manner that engenders trust by the warfighter. Second, the context in which DOD operates means these technologies are prone to adversary attack and system failure, with very real consequences. Machine learning systems have an increased potential for failure modes relative to other systems, such as bias due to a distribution shift in data, as well as novel vulnerabilities to attacks ranging from data poisoning to adversarial attacks. One could easily imagine an image classifier that accidentally classifies a civilian school bus as a tank or an adversary exfiltrating a model processing sensitive intelligence, surveillance, and reconnaissance or communications data. Image classification algorithms developed for one environment (e.g., the desert) could turn out to work incorrectly in another environment (e.g., cities).*"[17]

To ensure that Marine Corps AI systems are reliable, resilient, and capable of performing under contested conditions, the Marine Corps has an increasing need to understand adversary threats to the development, employment, and sustainment of these systems in operational contexts. Besides providing a general threat awareness overview, this Appendix is intended to introduce considerations for a variety of on-going and potential actions to identify and mitigate adversary threats to AI employment, including:

- Expand education, training, experimentation and exercises to enhance understanding of performance attributes of own-force AI systems and mitigating the threats posed to them by adversaries.

- Develop intelligence and counterintelligence requirements to address threats to the AI acquisition process and protect the supply chain.
- Develop and deploy risk-worthy AI and autonomous systems suitable for use where loss or compromise of some hardware is likely. Provide associated Security Classification Guidance and policy enabling informed risk decision-making.
- Establish and update AI test, evaluation, validation, and verification processes.
- Develop of operational data management systems and practices to enhance and protect Marine Corps AI capabilities.
- Develop intelligence and counterintelligence requirements to counter adversary capabilities to deny, degrade, disrupt, deceive or otherwise defeat Marine Corps employment of AI capabilities.
- Incorporate the status of key AI systems training, testing, validation, and operational performance into Commander's Critical Information Requirements (CCIR) and other reporting requirements.
- Incorporate requirements to protect friendly AI capabilities into operational activities for cybersecurity and information assurance, OPSEC, deception, Force Protection, Counterintelligence (CI), and Counter- Intelligence, Surveillance, and Reconnaissance (C-ISR) operations.

Threat Assessment Framework

Adversary attacks on Marine Corps AI-enabled systems can be aligned against three broad categories. Integrating AI capabilities into a military system introduces new vulnerabilities specific to the AI itself. ***Adversarial AI*** is a new category of threat that seeks to attack the functionality or performance of the AI itself.[18] A second category of threat is posed through a traditional ***Target Systems Analysis*** approach where the adversary seeks to attack vulnerabilities in the larger system or infrastructure which then precludes the Marine Corps from gaining advantage from the AI. A third category to consider is ***Systems Overmatch***, where a peer adversary applies their AI capabilities to gain some superiority over friendly AI systems. These threats may also be integrated as combined arms for increasingly ***Complex Operational Threats***. This framework will consider adversary use of AI capabilities specifically to counter Marine Corps AI systems but is not intended to be a more comprehensive assessment of all threats posed by adversary use of AI and autonomous systems.

As a new threat inherent to the adoption of Marine Corps AI systems, Adversarial AI should be understood and further integrated within functional threat assessments and risk mitigation activities. It is different than many conventional threats in that it does not directly attack system infrastructure or known vulnerabilities. Rather, Adversarial AI acts against the very features of AI and machine learning processes that makes it useful; how the AI system uses data inputs to act and to learn from results to improve its performance. MITRE ATLAS (Adversarial Threat Landscape for Artificial-Intelligence Systems) framework defines three basic paths for Adversarial AI attack: ***AI Access Time, AI Access Points, and System Knowledge***.[19] AI Access Time refers to actions addressing the internal processing of the AI infrastructure first to train an AI model, and then use the AI model to generate operational outputs. Consequently, this type of attack entails adversary access into the AI system itself, most typically either via cyber operations or insider threat activities. AI Access Points considers attack via external inputs to an AI system. These external inputs may be via a digital interface or physical interactions. An adversary may attack an AI system through a digital interface such as an API to send commands or queries and observe the response. An adversary may also present or manipulate data in the real world to observe or influence an AI system's behavior. System Knowledge broadly reflects adversary actions based on their understanding of AI system performance and ability to predict its response to a given input. In this case, an adversary could apply System Knowledge to stimulate a response from the AI system that is harmful. This can range from causing unintended damage to simply being overly predictable and subject to exploitation.

It is critical to consider adversary threats holistically across the AI lifecycle of development, employment, and sustainment. While the basic paths for Adversarial AI are relevant across each phase, persistent and evolving threats may apply a variety of tactics specific to each phase. This is true both within the consideration of Adversarial AI, but also how an adversary may integrate these tactics with the other concepts of Target Systems Analysis, Systems Overmatch, and Complex Operational Threats. Comprehensive threat analysis by phase is necessary to adequately inform development threat mitigation strategies.

Development Phase

Primary adversary activities during the development phase may include efforts to gain access to and knowledge of AI systems, including architecture, components, processes, and performance. While the PRC is perhaps the most capable, a host of adversaries seek to gain access to the AI systems development.[20] This may be to advance their own capabilities, undermine ours, or simply gain a better understanding of system performance parameters.

Adversarial AI against Access Time:

- o Any adversary access to the development environment and training data poses foundational risks to AI systems. For example, "data poisoning" is a well-documented Adversarial AI technique where training data is modified, such as by injecting false information or otherwise fine-tuning datasets to undermine the accuracy and reliability of operational outputs. Adversaries exploit these weaknesses by injecting false information into training datasets, undermining the accuracy and reliability of operational outputs. For instance, even relatively minor changes to a compromised dataset could cause AI systems to misclassify targets or misinterpret critical signals, directly affecting mission success.[21]

- o These efforts may also enable staging backdoor access for future exploitation or attack. For example, in an operation known as "Cloud Hopper," the cloud services of IBM and other U.S. defense contractors were penetrated by Chinese hackers from the Ministry of State Security.[22]

- **Adversarial AI based on Systems Knowledge:** If unable to gain full access to the development environment, an adversary may also seek to gain an approximate understanding of the AI system by replicating training data and/or obtaining models to serve as proxies for the target model. An adversary would then use the proxy models to simulate complete access to the AI system and support further evaluation of prospective capabilities and vulnerabilities.

- **Enabling Adversarial AI Attacks:** Reliance on global supply chains introduces significant risks, particularly from adversarial state actors like China. Economic coercion, intellectual property theft, and hardware tampering present clear pathways for adversaries to compromise AI systems before they are even deployed.[23]

Employment Phase

Once operational, AI systems face a variety of Adversarial AI threats, as well as those posed by the target systems and systems overmatch approaches.

- **Adversarial AI against Access Time:** An adversary who has previously gained direct access to the AI system could conduct a backdoor attack to interfere with system performance and output. Similarly, there are multiple tactics available to an attacker who has gained a digital interface with the AI system such as via a network connection. These actions include providing adversarial data inputs or queries which can overload system processing, create "chaff" which increases the need for manual review of system outputs, or otherwise degrade AI system performance. These tactics are ultimately intended to degrade AI system performance and undermine confidence in its effectiveness.

- **Adversarial AI against Access Points:** Even without direct digital access to an AI system, an opponent may take actions in the physical environment to conduct Adversarial AI attack. Just as camouflage can obscure visual observation by a human, minor changes to an object can likewise dramatically affect perception by an AI system. Referred to as a perturbation, this kind of attack can be imperceptible to a human observer. AI processing of other data sources, such as from electromagnetic receivers and audio/acoustic sensors may be similarly susceptible to this kind of adversarial AI attack.[24] In the case of AI systems processing data in the information environment, such as social media content, an adversary may use their own AI and automation capabilities to create adversarial attacks that are ingested by data collection efforts. Some examples of these kinds of attacks include: indirect introduction of malicious prompts to a large language model used by a Marine Corps AI system; tailored data designed to stimulate a desired response from the AI system; and presentation of large volumes of disinformation intended to undermine model performance.[25] In some cases, the purpose of attack may not be exclusively to undermine the model. Adversaries may provide inputs which reveals properties of training data as a whole or even allows the attack to reconstruct the specific training data. This can pose an additional threat when classified or otherwise sensitive information used as training data.[26]

- **Adversarial AI based on Systems Knowledge:** Every effective attack or counter to an AI system is predicated on some level of systems knowledge, whether specific to the system or more generalized. However, unlike the above examples targeting AI performance via access time and access points, an adversary who can develop insights into system performance may identify exploitable vulnerabilities. This is no different than how spammers adjust their format and content to circumvent email filters or how military forces adjust tactics such as attacking at night or flying at low altitudes to exploit gaps in adversary sensor capabilities. An AI system processing video feeds may perform better when detecting and classifying objects in one biome than another. Very generally, the more precise a desired output is, the more opportunity there is for the AI to make errors in its classification. AI systems may have identifiable bias or other patterns which can result in predictable outputs when presented with certain inputs or conditions. Some AI systems may have an exploitable delay in processing data to generate an output due to the volume of data, limits in processing capacity, or latency in an associated communications network. AI systems adopted by the Marine Corps will have performance trade-offs. The need for the Marines using these systems to understand their operating parameters and associated vulnerabilities is no different than any other weapons system.

- **Target Systems Analysis against AI systems:** In addition to the new and unique threats posed by Adversarial AI, any assessment of Marine Corps AI systems must also consider the full range of vulnerabilities and dependencies posed by an adversary, particularly during heightened competition through open conflict.
  - Depending on the system, it may have dependencies on data processing capabilities, whether cloud-based distributed resources, individual data centers, or expeditionary nodes. For instance, the "Cloud Hopper" operation demonstrated how adversarial actors exploit

cloud infrastructure vulnerabilities, enabling access to critical systems and data.[27] At the other end of an AI-enabled process, an adversary may act to deny us necessary data, such as through signature management or by shutting down civilian voice and data networks in a region. These elements (sensors, processing, and decision-making) and the associated connections between them may be susceptible to cyberattack, Electromagnetic Spectrum (EMS) interference, or physical destruction. Adversary operations in the information environment may employ AI-enabled narratives to distort perceptions, amplify confusion, and degrade operational coherence.

  - Central to any comprehensive analysis of an AI system is evaluation of how Marines employ the system, including its interaction with human cognition. Adversaries can seek to exploit gaps in human trust, understanding, and oversight of AI Systems. Adversarial AI attacks may serve to build operator distrust in the AI system by requiring that operator to spend significant time manually checking results and updating models or data sets to correct outputs. The goal is to influence Marines to ultimately abandon use of the AI system and negate any prospective advantage. Alternatively, adversary exploitation of insufficient understanding and oversight of AI systems can allow them to create exploitable gaps no different than uncovering a gap in air defense radar coverage or sleeping sentry. Effective use of AI systems necessitates that the humans employing these capabilities understand AI performance parameters to benefit from its capabilities. This understanding what the AI systems can and cannot do well, as well as recognizing when there is any variation in expected performance enables detection of adversarial actions.

- **AI Systems Overmatch:** AI and autonomous system capabilities are being broadly adopted by the defense industry in several nations and appearing to varying degrees in on-going conflicts.[28] The conflict between Russia and Ukraine has highlighted the iterative development and implementation of these capabilities by both sides.[29] The competition to deploy ever-increasing amounts of AI-enabled and autonomous systems is already lead to engagements between unmanned and AI-enabled systems. Recent PRC studies on the U.S. Replicator Initiative have highlighted its efforts to deploy swarms of autonomous systems to counter their numerical superiority in conventional weapons systems. However, PRC commentary also suggests confidence in their ability to overwhelm U.S. autonomous systems through superior production of AI and autonomous systems combined with sophisticated EMS countermeasures.[30] To that end, the PRC has implemented state-funded initiatives to mass-produce low-cost autonomous systems. In 2024, a PRC drone light show company set world records for the most airborne multi-rotor drones to be controlled from a single computer and largest aerial drone light show during a remarkable display of nearly 10,200 quadcopters.[31] While not explicitly a military capability, this demonstration highlights the ability of the PRC to marshal large amounts of AI-enabled robots. This technology is widely available at such low cost such that even an otherwise marginal adversary may find it possible to marshal a tactically significant amount of such weapons to achieve overmatch at a specific location.

Sustainment Phase

Any AI System which is employed over time must also be evaluated in terms of the threats and vulnerabilities to its prolonged use in the dynamic and often chaotic environment of combat. Maintaining AI systems over time requires continuous monitoring of system performance and training with new data to address shortfalls and build on success. Adversarial AI attacks must be countered while associated networks and development environments are defended. Long-term use of AI systems -- absent continuous updates to data sets and models -- can lead to degraded performance and unexpected behaviors. Even if

AI systems are properly maintained, their sustained use will likely lead to increased adversary familiarity with their capabilities. These conditions can enable an adversary to pose increasingly complex operational threats.

- **Complex Operational Threats:** Adversaries will seek to leverage multi-domain combined arms tactics that integrate a variety of threats in an integrated manner. The PRC's focus on "intelligentization" represents a strategic shift to integrate AI for decision-making autonomy, swarm tactics, and AI-enabled psychological operations.[32] This approach, described in Chinese literature as "Systems Destruction Warfare," emphasizes degrading adversary systems through interconnected attacks on personnel, platforms, and munitions.[33] For instance, adversarial swarming tactics, involving large formations of autonomous systems, can overwhelm defenses through sheer numbers and dynamic decision-making, creating chaos and reducing the effectiveness of traditional countermeasures. The effectiveness of these swarms can be further enhanced through simultaneous adversarial AI, cyberattacks, EMS jamming, and physical attack of key nodes and networks. These coordinated strategies aim to exploit interdependencies between domains, such as disabling communication systems while targeting physical infrastructure. Additionally, adversaries will attempt to manipulate human and AI decision loops by introducing disinformation or spoofing attacks, leading operators to question system outputs – or trust erroneous outputs. When applied as part of a complex multi-domain combined arms attack, these efforts against human-machine teaming and cognition can undermine the accuracy and timeliness of decision-making at all echelons, potentially to devasting effect.[34]

Conclusion

Adoption of AI and increasingly autonomous systems by the Marine Corps poses great opportunities to enhance operational effectiveness while reducing the risk to humans in combat. Nonetheless, implementation of new capabilities also introduces unique new vulnerabilities, all of which must be continuously assessed and mitigated. These vulnerabilities are further magnified if AI and autonomous systems are employed without the requisite understanding of system performance and required upkeep to properly fight these complex systems. This Appendix is intended to be used as an overview framework for more substantive assessments of adversary threats to each specific AI system. Consequently, it also highlights the need to develop corresponding intelligence and counterintelligence requirements to further identify and mitigate adversary activities and threats.

[16] https://www.nist.gov/itl/ai-risk-management-framework

[17] https://cset.georgetown.edu/wp-content/uploads/Building-Trust-Through-Testing.pdf

[18] https://www.paloaltonetworks.com/cyberpedia/what-are-adversarial-attacks-on-AI-Machine-Learning

[19] https://atlas.mitre.org/resources/ai-security-101

[20] "Protecting Critical and Emerging U.S. Technologies from Foreign Threats," The National Counterintelligence and Security Center, Oct 2021.

[21] "U.S.-China Competition and Military AI," Center for New American Security. https://s3.us-east-1.amazonaws.com/files.cnas.org/documents/FINAL4.pdf

[22] https://warontherocks.com/2022/05/how-ai-would-and-wouldnt-factor-into-a-u-s-chinese-war/

[23] "PRC Views on the DOD Replicator Initiative," Vandegrift Team (VT) Red Report 20241007 (Unclassified)

[24] "The Navy Must Learn to Hide from Algorithms," U.S. Naval Institute. https://www.usni.org/magazines/proceedings/2022/may/navy-must-learn-hide-algorithms

[25] https://atlas.mitre.org/matrices/ATLAS

[26] https://www.techtarget.com/searchenterpriseai/tip/Adversarial-machine-learning-Threats-and-countermeasures

[27] https://warontherocks.com/2022/05/how-ai-would-and-wouldnt-factor-into-a-u-s-chinese-war/

[28] "Between Killer Robots and Flawless AI: Reassessing the Military Implications of Autonomy," Center for European Policy Analysis. https://cepa.org/article/between-killer-robots-and-flawless-ai-reassessing-the-military-implications-of-autonomy/

[29] "Battlefield Drones and the Accelerating Autonomous Arms Race in Ukraine," The Modern War Institute. https://mwi.westpoint.edu/battlefield-drones-and-the-accelerating-autonomous-arms-race-in-ukraine/

[30] "PRC Views on the DOD Replicator Initiative," Vandegrift Team (VT) Red Report 20241007

[31] https://www.guinnessworldrecords.com/news/commercial/2024/10/a-dazzling-display-chinas-record-breaking-drone-spectacle-with-over-10000-drones

[32] "U.S.-China Competition and Military AI," Center for New American Security. https://s3.us-east-1.amazonaws.com/files.cnas.org/documents/FINAL4.pdf

[33] "Systems Confrontation and System Destruction Warfare," Rand. https://www.rand.org/pubs/research_reports/RR1708.html

[34] ECSM 018 Marine_Corps Assessment and Authorization Process V7.0, dtd 24 Jan 2024

Appendix H: AI Implementation Roadblock Assessment

This Appendix outlines major challenges to implementing AI across the Service as a result of the assessment MIU conducted with key leaders and stakeholders.

Centralized Authority to Operate Process

Limitations:
A significant issue the Marine Corps faces in implementing AI across the force is a lack of speed and agility in the ATO process. While MCO 5230.21, Information Technology Portfolio Management, ECSM 018, and the most current IRM 2300-19 Marine Corps IT Registration Policy already outline the ATO process, there are current two Authorizing Officials (AOs) to sign off on all software, from enterprise applications to tactical networks.

Recommendations:

1. Assess for opportunities to increase the speed and agility of the ATO process.

Risk Management Framework

Limitations:
The Marine Corps' implementation of the Risk Management Framework (RMF) faces challenges in keeping pace with evolving software technologies. Continuous monitoring presents particular challenges when applied to AI models that require constant updates and retraining to stay relevant, in some cases retraining models multiple times in a day.

For the Marine Corps to implement AI effectively, it must adapt the RMF process to account for the unique risks posed by AI. One solution is to separate the evaluation of AI models from the standard software environment assessments. The runtime environments for AI models can still execute the traditional RMF process, but the security and validation of AI models will require a distinct pathway that addresses issues such as model drift, data leakage, and other AI-specific considerations.

Another critical point is the need for better data rights management within the AI development pipeline. Currently RMF procedures may not fully address data security posture management (DSPM), leading to vulnerabilities in AI systems. Tools like Varonis and Immuta could be integrated to improve visibility over data use, ensuring that AI models are trained on secure, compliant data.

Recommendations:

1. Leverage existing NIST AI RMF 600.1 "Artificial Intelligence Risk Management Framework" and USMC RMF (DRAFT) to include a distinct evaluation pathway for AI models
2. Expand the use of Interim Authority to Test (IATT) for AI projects and collaborate with other DoD AI security divisions and programs to refine and accelerate RMF processes.

Fragmented Data Management Across the Service

Limitations:
Perhaps the most significant challenge to AI implementation is the fragmentation of data across the Marine Corps. Different units manage their data independently, leading to inconsistencies in how data is stored, accessed, and used. This fragmentation may present challenges for developing AI tools that rely on real-

time data. The Marine Corps can maximize its potential for AI success by adopt a data federation strategy that allows secure, real-time access to relevant data across units. The Marine Corps should consider implementing a data fabric architecture to effectively connect data across a multi-cloud, on premises, and on device environment.

Zero Trust Architecture is a key principle that should underpin any AI deployment, and DSPM is critical to reducing data leakage, especially for sensitive AI applications. The Marine Corps should integrate attribute-based access controls (ABAC) and other security mechanisms to ensure that data is only accessible to those who need it, when they need it. By following the USMC Zero Trust Implementation Plan, the Corps can reduce the risk of cyber-attacks and data breaches, which are particularly harmful in AI environments.

The security of training data also requires special attention. AI models rely on vast datasets for training, and these datasets often contain sensitive information. Training data should be treated as more secure than production data, given the impact that corrupted or compromised data could have on AI model behavior.

Recommendations:

1. Implement a data fabric strategy to provide data federation with storage solutions, consistent data tagging, data lineage, and data ownership to enable secure, real-time data access.
2. Underpin AI deployments with Zero Trust architecture by integrating ABAC and establishing policies for data security.
3. Establish policies for handling training data, including access controls and encryption standards to ensure the integrity and security of AI models.

Outdated Cultural Approach to Building, Deploying, and Managing Software

Limitations:

Currently, the Marine Corps does not have a platform for AI development. Each unit that embarks on an AI project often builds its infrastructure from scratch, including cloud contracts, software testing environments, and pipelines. This approach can lead to duplication of effort and slows down the process of obtaining an ATO. A shared platform can alleviate these challenges.

One solution is to develop an enterprise AI platform to serve as the foundation for all Marine Corps AI projects. By building this platform, the Corps could reduce ATO-related friction, allowing developers to focus on building solutions rather than infrastructure. Platforms like ADVANA and the Army's Platform One have proven successful in providing shared infrastructure for AI development.

An Enterprise DevSecOps Solution could greatly speed up AI development by standardizing how software is built, tested, and deployed across the Marine Corps. A serverless platform would be an ideal solution for the Marine Corps, enabling developers to build and deploy software while abstracting away underlying infrastructure. This could empower bottom-up software solutions tailored to specific needs.

Recommendations:

1. Develop a standardized, shared AI development platform to eliminate redundant infrastructure efforts and expedite the ATO process, leveraging successful models.
2. Realign structures to reward efficiency and agility in smaller projects, promote DevSecOps practices, and foster a cultural shift toward innovation and adaptability in AI initiatives.

3. Investigate the feasibility of introducing a serverless platform for AI development, potentially modeled after Azure’s cloud environment, to empower developers and streamline the development process.

Conclusion: Building a Foundation for AI Success

To fully realize the potential of AI, the Marine Corps must make significant adjustments to its procedures and culture. By assessing the ATO process, streamlining RMF procedures for AI, adopting a shared platform approach, improving data federation and security, and fostering a cultural shift toward agility, the Corps can position itself at the forefront of AI policy and implementation. These changes will enable faster, more efficient development of AI tools, ultimately enhancing the Marine Corps' readiness for the *future fight*.

Appendix I: AI Integration with the Cybersecurity Framework

The rise of AI is transforming cybersecurity, providing new tools to combat evolving threats. This AI Cybersecurity Framework aims to harness AI's potential to strengthen defenses while navigating technological, ethical, and privacy challenges. As our world becomes increasingly interconnected with data flows across global networks, robust cybersecurity is more critical than ever. AI's ability to learn, adapt, and predict makes it an invaluable tool against cyber threats like sophisticated malware and phishing attacks. However, integrating AI into cybersecurity also raises concerns, including data privacy and AI-driven threats. This framework outlines a strategy that leverages AI's strengths while mitigating its risks, to ensure a resilient and ethically sound cybersecurity approach. By setting a standard for AI-driven cybersecurity, this framework encourages innovation, collaboration, and provides a model for others to follow in the pursuit of cyber resilience.

Threat Landscape

The cyber threat landscape is rapidly evolving, with AI introducing new dimensions to both cyber threats and defenses. Adversaries are increasingly utilizing AI to automate attacks, enhance phishing and social engineering tactics, and develop malware that can adapt and evade traditional detection methods. Our framework addresses these challenges, leveraging AI's potential to enhance threat detection, response, and prediction, while mitigating its risks and ensuring a resilient cybersecurity posture.

Ethical and Legal Considerations

The integration of AI into cybersecurity brings to the forefront a complex array of ethical and legal considerations. Ethically, the use of AI in cybersecurity must balance the imperatives of effective threat mitigation with the fundamental principles of individual privacy and data protection. Legally, the framework must align with international and domestic laws, including evolving regulations around data sovereignty, cross-border data flows, and AI governance.

Privacy and Data Protection Policies

The approach to AI-driven cybersecurity is built on several key pillars, including a commitment to privacy and data protection, adherence to ethical and legal considerations, and a focus on technological innovation and infrastructure development. It prioritizes research and development recognizing the importance of staying ahead of the evolving cyber threat landscape through continuous innovation and collaboration.

Technology and Infrastructure

The framework emphasizes the importance of a resilient infrastructure, including high-performance computing resources, scalable cloud computing solutions, and secure and reliable data storage systems. The combination of cutting-edge AI technology with a strong, adaptable infrastructure is the cornerstone of a resilient and effective AI Cybersecurity framework.

Research and Development

In the rapidly evolving domain of AI and cybersecurity, a robust and proactive Research and Development (R&D) strategy is vital. The approach is centered on fostering innovation and staying ahead of the sophisticated cyber threat landscape through continuous R&D efforts. Creating dedicated R&D facilities and testbeds that provide a safe environment to simulate real-world cyber attacks and assessing the effectiveness of AI-driven defense mechanisms is important.

Workforce Development

Investing in the workforce, enhances the cybersecurity capabilities and builds a sustainable talent pipeline that can adapt to and manage the future landscape of cyber threats augmented by AI technologies. The focus on workforce development is not just an investment in skills but a foundational pillar for a resilient, dynamic, and innovative cybersecurity future.

Risk Management

Effective risk management is paramount in the AI Cybersecurity framework, addressing the unique challenges and vulnerabilities introduced by AI technologies. AI systems, while powerful, are not infallible, and the approach focuses on identifying, assessing, and mitigating risks proactively. The risk management framework includes stringent data governance measures to safeguard against unauthorized access and data breaches, ensuring compliance with privacy laws and ethical standards.

Conclusion

In conclusion, the AI Cybersecurity framework represents a comprehensive approach to addressing the challenges of the digital era. At its core, this approach recognizes the transformative potential of artificial intelligence as a pivotal ally in the battle against cyber threats. It aims to harness AI's capabilities to enhance the defensive mechanisms and anticipate future cyber risks, with a commitment to ethical and legal adherence, robust technology, and infrastructure investment. The successful implementation of this framework requires a concerted effort across multiple domains, including fostering a skilled workforce, continuous research and development, and effective risk management. The approach emphasizes vigilance and adaptability, preparing for the evolving nature of cyber threats. This framework is a commitment to innovation, collaboration, and excellence, positioning to lead in cybersecurity and face current and future challenges in an increasingly interconnected world.

Appendix J: AI and Analytical Maturity Model

The AI and Analytical Maturity Model (AIAMM) outlines a progression of capabilities from basic data management to advanced analytics and AI. It is important to recognize that the goal is to support data-driven decision-making through strategic insights, which can be achieved by many means—not solely through AI. AI tools are one potential enabler at the most advanced stage of this model, but they are not the only route to sophisticated and effective analysis. The five-level maturity model is as follows:

1. **Foundational Data Management:** At this initial stage, organizations focus on establishing robust data management practices. This includes collecting, storing, and maintaining data in a structured manner. Key activities involve data governance, quality assurance, and basic reporting to ensure data accuracy and reliability, including mapping data to specific attributes. These practices provide the critical infrastructure needed for all subsequent analytical efforts.

2. **Descriptive Analytics:** As organizations mature, they begin to use data to understand what has happened. This stage involves summarizing historical data to identify trends and patterns. Tools such as dashboards and reports are employed to provide insights into past performance. Importantly, these techniques support effective decision-making without requiring advanced algorithms or AI.

3. **Diagnostic Analytics:** Building on descriptive analytics, organizations then delve into understanding why certain outcomes occurred. This stage utilizes statistical analysis and data mining techniques to uncover the root causes behind trends and anomalies. The insights gained at this level help in identifying the factors influencing performance, paving the way for more informed decisions.

4. **Predictive Analytics:** At this stage, organizations leverage advanced analytics to forecast future trends and outcomes. Predictive analytics uses historical data to build models that anticipate future events, thereby enabling proactive planning and strategy formulation. It is crucial to note that while machine learning techniques—including some AI applications—can be used here, predictive analytics can also be achieved through a range of statistical methods and other analytical approaches.

5. **Prescriptive Analytics and AI-Enabled Decision Making:** The most advanced stage integrates prescriptive analytics with AI to not only forecast future events but also to recommend actions. Organizations at this level may use machine learning algorithms, natural language processing, computer vision, and other AI technologies to optimize processes and drive innovation. However, the use of AI in this context is an enabler that enhances analytical capabilities rather than being the sole driver of strategic insights. The focus remains on achieving effective, data-driven decisions through the best combination of available analytical tools.

Each level of this maturity model represents a significant advancement in an organization's ability to derive strategic insights from data. The AI IPlan supports all levels, ensuring that while AI can provide powerful capabilities at the highest level, robust analytics practices at every stage are essential for effective decision-making. This approach emphasizes that the strategic, data-driven insights at the heart of successful decision-making are not dependent solely on the use of AI.

Appendix K: ETMS2 Staffing Summary

This appendix provides the General Officer, Flag Officer, and Senior Executive Service (GO/FO/SES) level concurrence of this AI IPlan which includes Service-wide tasking. The associated Enterprise Task Management Software Solution task ID numbers are provided as reference for each round of official staffing.

AO level review was completed via tasker ID # DON-241031-WFHX on 22 Nov 24.
O6/GS15 level was review completed via tasker ID # DON-241216-9QRF on 22 Jan 25.
GO/FO/SES was level review completed via tasker ID # DON-250303-54RZ on 28 Mar 25.

Below is a complete listed of the GO/FO/SES responses received from the primary OCRs tasked via ETMS2:

Owner	Role	Response
USMC DC I SDO	Initiator	
USMC DC A	OCR	Concur with implementation. No additional comments.
USMC DC CDI	OCR	CDD Concurs with comments.
USMC DC I	OCR	Reviewed and concur with recommended comments.
USMC DC IL	OCR	Concur without comment.
USMC DC MRA	OCR	Concur with comments.
USMC DC PPO	OCR	Concur with comments.
USMC DC PR*	OCR	Non-concur, with comments.
USMC TECOM	OCR	Concur with comments.
USMC MCSC	OCR	Concurs with the Plan without comment.
USMC MarForCom/MarForNorth	OCR	Concur. No comments
USMC MARFORRES	OCR	Concurs without comment.
USMC MFP	OCR	Concur without comments.
USMC MFE/A	OCR	Concur without comments.
USMC MFK	OCR	Concur as written.
USMC MARFORSOC	OCR	Concur with comments.
USMC MARFORSPACE	OCR	Concur with comments.
USMC MARFORCYBER	OCR	Concur with comments.
USMC PEO LS	OCR	Concur without comments.
USMC HQMC CD 45OFS	OCR	Concur with no comment.

The non-concur received from DC P&R was due to a conflict of interest with DC P&R's inclusion in developing a cost estimate via Task 3.3.2. DC P&R was removed from this task and has acknowledged that this resolves their non-concur.