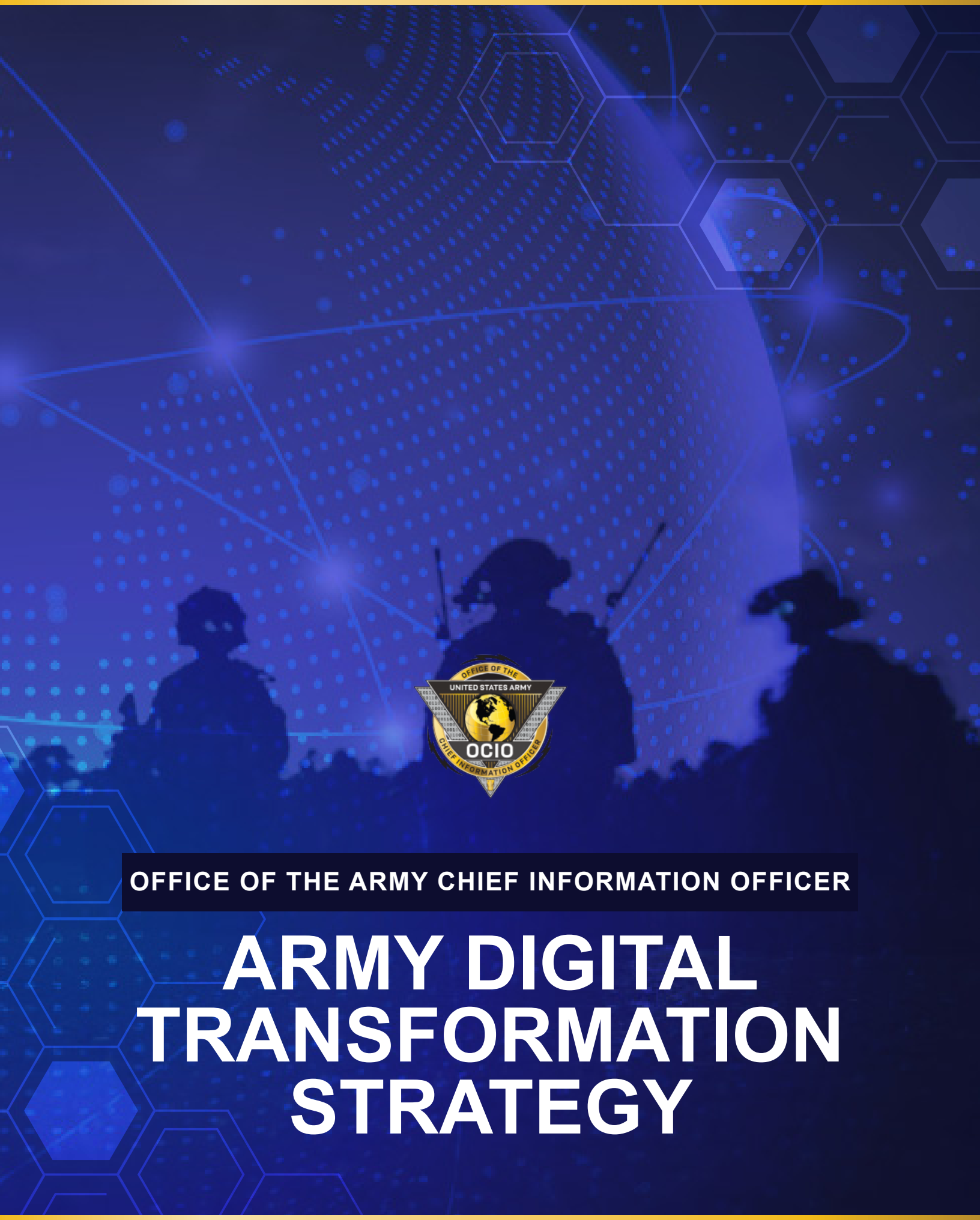


OFFICE OF THE ARMY CHIEF INFORMATION OFFICER

# ARMY DIGITAL TRANSFORMATION STRATEGY

**Headquarters,**
**Department of the Army**
**12 October 2021**

# Army Digital Transformation Strategy

**DISTRIBUTION STATEMENT A:**
Approved for public release, distribution is unlimited

# THE JOURNEY TO ARMY WAYPOINT 2028

As the Army marches toward its goals of being a more ready, lethal, and modern force by 2028, it faces unprecedented challenges in modernizing its platforms and weapons systems, but also its business processes and workforce to dominate adversaries on and off the battlefield in multi-domain operations (MDO).

The Army Digital Transformation Strategy (ADTS), established by the Office of the CIO, is the overarching framework that will set the vision, establish lines of effort (LOE), and implement strategic digital transformation initiatives prioritized and resourced as required to achieve this end state. Each LOE and initiative must be outcome driven to ensure that it is operationally effective in a resource constrained future.

The Army must and will make bold investments in transformative digital technologies, build the workforce into one with the training and experience to execute the full range of Army missions in increasingly complex technological environments, and put the right data in decision makers' hands quicker than ever before.

The Office of the CIO will lead these efforts for the Army in partnership with Headquarters, Department of Army (HQDA), Army Commands, Army Service Component Commands (ASCCs), Direct Report Units (DRUs), the DoD CIO and Joint Staff, and Allied Nation Partners as required.

Christine E. Wormuth
*Secretary of the Army*

## STRATEGIC INTENT

The adoption of leading edge technologies by the Army's and the United States' near-peer adversaries, combined with the rapid pace of change in technology, is creating new and complex challenges for how the Army operates and maintains overmatch across all domains – land, sea, air, space, and cyberspace. As the Army responds to the growing need for digital technologies through Army modernization programs, the cybersecurity attack surface area is growing exponentially, and the dynamic threat environment requires the Army to make fundamental changes to address security in all phases of the lifecycle to ensure the Army is poised for defensive and offensive cyber operations. The Army must adapt a data-driven mindset and embrace digital transformation to successfully respond to the threat of great power competition and win decisively in a Large Scale Combat Operations through MDO.

The Army Modernization Strategy identifies digital transformation as the means to modernize the Army to achieve Waypoint 2028 and Aimpoint 2035. Digital transformation represents a shift in operations and culture that fundamentally changes how an organization delivers value through the adoption of advanced technologies such as cloud, data and artificial intelligence (AI). Digital transformation is driven through innovation and new business and operating models, powered by a digital workforce that is agile, adaptive, and tech-savvy. Digital transformation is an enabler for Army readiness and reform and serves as a catalyst to revitalize and establish the Army's digital workforce of the future. The Army must keep pace with the rapid change in technology, adopt modern best practices, and avoid any delays from bureaucratic institutional processes. The Army must make bold investments in transformative digital technologies, reform its institutional processes, and build its workforce into one with the training and experience to execute in increasingly complex operational environments with the technological innovation that places the right data in decision makers' hands quicker.

The Army must accomplish digital transformation in a fiscally constrained future. To accomplish this, reform efforts are needed to continually assess the Army's digital portfolio, explore opportunities for divestment of legacy systems, re-engineer business processes, adopt greater automation, and find savings through consolidation and better buying power. The cost avoidance harvested from such reform efforts can be re-allocated to modernize enduring legacy systems, data, and networks to achieve even greater cost savings in the future.

Army will improve on how it executes institutional processes such as requirements development, acquisition, Planning, Programming, Budgeting, and Execution

### DIGITAL TRANSFORMATION

…investing in ***digital transformation*** and the modernization of the Army's underlying network and computer infrastructure is essential to our success. Specifically, the ***cloud is the foundation for this entire modernization effort.*** The Army will develop cloud computing technologies, ***improve data access and sharing environments***, and ***streamline software development tools and services***. Together, these technology investments will allow the Army to take advantage of emerging machine learning and AI technologies to understand, visualize, decide, and direct faster than our competitors. By leveraging cloud open architecture, information can flow rapidly between the enterprise and soldiers on the ground. This will enable commanders to counter adversaries in the information environment as effectively as they do in physical domains and win in the cognitive space.

***Source: Army Modernization Strategy, 2019***

(PPBE), and talent management. Digital transformation requires an outcomes-based, metrics-driven mindset to measure activities and to continually seek efficiencies and effectiveness. The ADTS will serve as the guiding document to inform changes to these processes which will enable the Army to more easily adopt digital transformation and mission effectiveness. The Assistant Secretary of the Army (Acquisition, Logistics and Technology) will continue to have oversight of acquisition, logistics and technology matters of the Department of the Army. In addition, as the Army Acquisition Executive, the ASA(ALT) is responsible for the management and control of the Army acquisition system.

Finally, digital transformation is aimed at developing an organic digital workforce of the future that can continually adapt and adopt new digital technologies, and is capable of applying these technologies to mission needs. In order to scale ongoing pilot efforts such as the Software Factory (an Army organization that trains and enables soldiers to produce modern software), the Army needs to change how it recruits, trains, and retains its digital workforce and reduce the gap between the organic and commercial workforce. This requires partnerships with allied nations, industry, and academia at scale as well as other tools to enable the workforce to grow and develop leading edge technologies.

The Office of the CIO is formalizing the ADTS to establish the vision for how digital transformation can help achieve the Waypoint 2028, indicate clear LOEs leading to this objective, identify priorities for the Army to resource, and outline an integrated master plan to synchronize and better integrate all ongoing activities to achieve a digital-age Army.

The scope of the ADTS covers all Title 10 mission areas as outlined in Army Regulation 5-1 [Warfighter Mission Area (WMA), the DoD portion of the Intelligence Mission Area (DIMA), the Enterprise Information Environment Mission Area (EIEMA), and the Business Mission Areas (BMA)], all Army Commands, DRUs, and ASCCs; all Army Components (the Regular Army, the Army National Guard of the United States, and the Army Reserve); all appropriation types; and both enterprise and tactical requirements supported by both the military and civilian workforce. The ADTS augments and aligns to other DoD and Intelligence Community strategic guidance such as USD(I&S), Director National Intelligence (DNI) and Defense Business System strategies.

## STRATEGIC ALIGNMENT

The ADTS fully aligns with wider Army, and DoD modernization strategies, which share the vision of a more ready, lethal, and modern force by 2028. While inputs were taken from an extensive list of documents, several key strategies provided significant direction for the ADTS and influenced the objectives, LOEs, and overall priorities outlined. ADTS objectives are organized to indicate their alignment with Army's strategic pillars: modernization and readiness, reform, people and partnerships.

### KEY DOD STRATEGIES

DoD Digital Modernization Strategy

DoD Capabilities Programming Guidance

### KEY ARMY STRATEGIES

Army Campaign Plan

Army Modernization Strategy

Army Business Modernization Plan

Army Planning Guidance

## ARMY DIGITAL TRANSFORMATION STRATEGY

### VISION

A digital Army of 2028 able to deliver overmatch through Joint Multi-Domain Operations (MDO) leveraging innovative and transformative technologies.

### MISSION

Drive digital transformation, innovation and reform through strategy, policy, governance, oversight and rapid capabilities to establish an operational MDO force.

***OBJECTIVE 1:*** **MODERNIZATION & READINESS**

A digitally-enabled, data-driven Army propelled by digital transformation

***OBJECTIVE 2:*** **REFORM**

Optimized and mission-aligned digital investments providing greater value to the Army

***OBJECTIVE 3:*** **PEOPLE & PARTNERSHIPS**

A tech savvy, operationally effective digital workforce partnered with a robust network of allies, industry, and academia

**ADTS advances the Army Modernization Strategy for Waypoint 2028 and Aimpoint 2035.**

## MODERNIZATION & READINESS

### OBJECTIVE 1:

***A digitally-enabled, data-driven Army propelled by digital transformation***

The Army's current digital initiatives are siloed across mission areas, inhibiting the interoperability needed to support MDO and Joint All Domain Command and Control (JADC2). The Army must prioritize resources for digital modernization over current year operational readiness. In addition, the Army should divest from unsustainable legacy systems while simultaneously investing in priority modernization efforts like cloud computing. Similarly, the Army should aim to balance resourcing IT service delivery and cybersecurity across the enterprise while also prioritizing modernization of the unified network. Between 2021 and 2028, the goal is to converge current digital initiatives that support readiness and modernization into a single integrated plan, enable these initiatives at the enterprise-level so they are available to the total Army from the tactical edge to the enterprise, and establish standardized service delivery processes, methods and tools, all fully leveraging cloud as an enabler. This effort will enable an Army that seamlessly shares data and information for timely insights to Warfighter, Commands, and enterprise functions, in direct support of Army readiness and modernization.

The following LOEs will drive both readiness and modernization objectives through the rapid adoption and implementation of digital technologies.

**LOE 1.1:** Accelerate cloud native adoption by unifying Army's enterprise and tactical clouds

The Army will adopt a "cloud smart" approach that supports the migration of enduring applications in existing Army Enterprise Data Centers (AEDC) and Installation Processing Nodes (IPN) to Army's cloud (cArmy) to achieve cost savings, interoperability, and information sharing across applications. The Army will establish the cArmy hybrid global cloud that is resilient, secure, and able to share computing and storage resources seamlessly for enterprise and tactical applications. All applications, as appropriate and excluding any Operational Technology (OT) systems, modernized to the cloud will adopt a DevSecOps methodology, enhanced to include non-traditional, but Army required security principles such as OPSEC indicator identification and data aggregation concerns, to shorten development lifecycles and build cybersecurity early in the design process. Army will adopt common cloud services to achieve standardization in cloud architecture, security monitoring, and transparency in cloud spending. The Army will prioritize use cases to support Project Convergence and MDO including tactical cloud pilots, threat capability red teams, and prototyping efforts across the Army and as appropriate with coalition and allied nation partners.

**LOE 1.2:** Leverage data as a strategic asset to achieve interoperability and data for decision making

The goal of this line of effort is to prioritize, mature, and scale ongoing data management efforts in order to leverage data for decision making across all echelons. An additional goal of this line of effort is to use the Enterprise Decision Analytics Framework/Enterprise Architecture (EDAF/EA) to validate interoperability across modernization programs that will support MDO through data standards and integrated operational, system, data, security, and technical architecture. HQDA governance will leverage real-time data from authoritative systems and dashboard capabilities through Army enterprise data integration platform for Army Senior Leader (ASL) decision making. System owners that house authoritative data will establish Application Programming Interfaces (API) for the curated and validated data and register them in the Enterprise Data Service Catalog (EDSC), as appropriate, for consumption by other enterprise users including feeds to Army enterprise data integration platform for DoD-level decision making forums. Use cases to support Project Convergence, JADC2, Army Prognostics and Predictive Maintenance, Mission Partner Environment (MPE), and Army modernization through the Common Operating Environment (COE) will be prioritized. Mission Areas and Commands will establish Data Stewards responsible for maintaining the quality of the data. The Army will unearth potential savings and cost avoidance opportunities in the current spending through net-new data analytics insights. The Army will establish standard accredited toolsets for AI, Robotic Process Automation (RPA) and Machine Learning (ML), as well as an enterprise data lake in Army's cloud for us by all mission areas. The Army will build an IT standards program that will assist all mission areas with building capabilities according to approved IT standards.

**LOE 1.3:** Elevate Army's cybersecurity posture by defining Zero Trust principles for both IT and OT assets

As adversaries continue to achieve greater sophistication in their offensive cyber capabilities, the Army must be able to protect its ever-increasing attack surface area of both traditional IT and non-traditional OT assets connected to the DoD Information Networks (DODIN) while still adopting commercial technologies. To achieve this, the Army will implement Zero Trust (ZT) principles for IT and OT assets by completing a current state assessment of ZT capabilities for all of its systems, rapidly addressing gaps in capabilities, implementing policies to integrate ZT into all aspects of Army processes including supply chains, and continually evaluating and maturing ZT across the Army. To enable Continuous Authority to Operate, the Army will rearchitect its networks, systems, and data to better take advantage of ZT principles and development approaches such as DevSecOps. The Army will fully implement Comply-to-Connect as part of the ZT Architecture to ensure that any device connected to the network is accredited and patched appropriately through compliance policies, and continually monitored to establish a trusted network. To establish seamless user access through a single credential, collaboration with allied nation partners, and to support financial audit requirements through separation of duties, the Army will implement a standardized enterprise Identity Credentialing and Access Management (ICAM) system to meet both enterprise and tactical/disconnected requirements , as well as mission-based Need-to-Know for all users. Finally, to proactively identify anomalous behaviors on the network, the Army must invest in and implement automated cybersecurity monitoring tools, automated red teaming tools, and big data analytics using AI.

**LOE 1.4:** Converge and modernize Army's IT infrastructure and networks

This line of effort will result in the Army removing barriers to efficiently deliver data, applications, and services that are needed to achieve multi-theater, multi-domain operations while at the same time establishing a predictable and resourced lifecycle tech refresh model for the networks. Today the Army's IT infrastructure and networks are not interoperable, not fully utilized, and require investments for tech refresh. In addition, because the organization networks (ORGNet) across the Army have not been converged, the Army is unable to manage the network as a unified network through standardized monitoring and Defensive Cyber Operations (DCO) tools. The Army will converge its 42 separate organization networks, rationalize and consolidate the network management tools supporting these networks, consolidate them into a single Active Directory, and optimize the unified network for MDO. The unified network will come under the oversight of U.S. Army Cyber Command (ARCYBER) for DCO enabling enable the Army to see, monitor and secure all assets (IT and OT) connected to the network. Through the Unified Network Operations (UNO) modernization effort, the Army will integrate the Integrated Tactical Network (ITN) and Integrated Enterprise Network (IEN) and leverage commercial technologies for transport, including 5G networking and Software Defined Networking (SDN). Leveraging these commercial technologies will enable high-speed, highly-available connections to the cloud and DODIN at lower costs. The Army will use ZT principles for the unified network and prioritize the network modernization for Secret Internet Protocol Router Network (SIPRNET) and secret releasable (SECREL) transport. Through Data Center Optimization, the Army will consolidate its enterprise and tactical compute and storage at its 12 AEDCs, 284 IPNs and other infrastructure to decrease current infrastructure by 50% in order to establish an integrated hybrid cloud capacity to maximize commercial cloud services while retaining capacity at AEDCs for resilience. In support of Army Installation Strategy (AIS), the Army will establish key standard operating architectures, models, and tools for IT and OT devices connected to the Installation Campus Area Network (ICAN) consistent with the mission of the installation tenant.

**LOE 1.5:** Converge and modernize Enterprise Business Systems

The end state of Enterprise Business Systems (EBS) modernization is a sustainment warfighting function that is a competitive advantage, fostering dominance in MDO with enabling technology and business processes. The Army's EBS – which serve as the business operations and management backbone for the Army – should aim to provide the Warfighter with the most modern capabilities available to execute sustainment or fiscal management operations, be interoperable with sustainment functions resident in current and future Warfighting Mission Area systems, and be compliant with the Global Force Management Data Initiative. To improve tactical, strategic, and audit readiness, the Army must modernize its EBS through Enterprise Business Systems – Convergence (EBS-C) and enable auditability to maintain transparency, traceability, and accountability. The Army will re-engineer its business processes to align with commercial best practices, threat mitigation best practices, and, where feasible, take advantage of commercial off-the-shelf (COTS) software capabilities. The Army will also establish an open technical architecture and open Application Programming Interfaces (APIs) for integration and interoperability in order to minimize vendor lock in and retain flexibility to adopt newer technologies in future. The Army will rationalize its Defense Business Systems (DBS) portfolio to eliminate legacy applications that are no longer effective or duplicative of existing capabilities. Applications to be subsumed by the modernized system must be placed in "break-fix" mode with critical security patching only while the modernized system is developed. The modernized cloud-native system will be developed using DevSecOps methodology, and enhanced to include non-traditional, but Army required security principles, to deliver incremental capability in deployable releases at least once every six months.

**LOE 1.6:** Drive mission-centric IT service delivery by defining standardized IT services

Since delivery of IT services is executed in siloed operations, the Army's technical debt and costs increase because different organizations and missions use variations of the same services, tools, and contracts to support similar services. To remedy this, the Army must standardize its IT service delivery by developing a new modernized enterprise service catalog that offers service levels consistent with the mission of the installation or unit. Army Commands and units will not be allowed to acquire "above baseline" services either as reimbursable or direct support. To support consistent and high quality service delivery, the Army will implement tools such as enterprise cloud-based IT Service Management (ITSM) that is accessible by all Commands, to enable U.S. Amy Network Enterprise Technology Command (NETCOM) to see, monitor and secure all assets on the unified network, and deliver end user support services integrated with IT Asset Management and IT Operations Management. The Army will standardize offerings of common open source analytics tools like Anaconda and R. Through ZT principles, the Army will provide greater support for Bring Your Own Approved Devices (BYOAD) and over time, divest from procuring government-furnished equipment (GFE) mobile devices and even laptops where feasible, in conjunction with expanded and robust Vendor Threat Mitigation programs across the Army. This will be accomplished by implementing Virtual Desktop Infrastructure (VDI) to enable users to securely access their desktop images from anywhere in the world remotely. The Army will also divest legacy unclassified Video Teleconferencing (VTC) and analog telephones with the enterprise implementation of a voice modernization strategy in conjunction with Army 365 collaboration capabilities. Legacy collaboration capabilities such as MilSuite, Army Knowledge Online (AKO) and Command level SharePoint instances will be divested to maximize the investment in Army 365. This will enable the Army to drive down technical debt and maximize its resources to more cost effectively meet mission needs. The Army will also reassess and validate services provided to Combatant Commands (COCOMs) as their Combatant Command Support Agency (CCSA) to ensure standardization and interoperability.

*"The Army must be manned, trained, equipped, and modernized to be ready to fight today, but also to meet the demands of an uncertain and unpredictable future."*

**— Honorable Christine Wormuth, Secretary of the Army**

**OBJECTIVE 2:**

***Optimized and mission-aligned digital investments providing greater value to the Army***

Operational excellence is an imperative for the Army in light of the tight fiscal reality in Program Objective Memorandum (POM) 2023-2027 and beyond. With the evolution of technology, commercial organizations are finding lower cost, more efficient, and innovative ways to run and invest in their enterprises. The Army seeks to maintain pace with the evolving advancement of technologies, but this requires a re-evaluation of priorities, resourcing, and investments. Current challenges include limited visibility into Army IT portfolios, inflexible and waterfall IT acquisition processes, and ineffective IT investment accountability and oversight. These challenges prevent the Army from ensuring its resources and spending are best aligned to save costs, improve operations, and ultimately harvest these savings to modernize the Army through digital transformation.

The goal is to optimize the Army's resources and enable confident investment decisions that are data-driven and objective while at the same time ensuring direct alignment of these investments to Army priorities. With agile institutional processes for acquisition, PPBE, and portfolio management, the Army can ensure better alignment of digital resources to current and future digital requirements. The following LOEs will reform the enterprise and drive the ability to optimize investments.

**LOE 2.1:** Optimize resource allocation and investment decisions by increasing visibility into portfolios

The Army must maximize the value derived from its digital transformation investments, which begins with transparency into all phases of the Army's PPBE process from planning through execution. The Army's PPBE process can be improved to gain better visibility over $15 billion annual digital spend allowing for better understanding of how this portfolio integrates to provide best value to meet the Army's priorities. To address this challenge, the Army must fundamentally reassess how the digital budget is addressed in the PPBE process. The Army will scale the TBM methodology across all portfolios and achieve granular insights into each investment through the PPBE process. This includes the coding of cyber capabilities in each investment to meet the requirements of reporting through the Principal Cyber Advisor to Congress. The Army will also mature Army digital resourcing visibility piloted in FY21 to a construct that enables the Army to validate, rationalize, and synchronize digital resource requirements, and prioritize digital investments to ensure that fully informed resource decisions are being made. The Army will continue to aggressively divest legacy systems through rigorous prioritization of the digital portfolios in each mission area. The Army will explore if the current mission area construct is optimal in the context of MDO and if changes are needed to enable greater synchronization and integration of the portfolios to breakdown silos between mission area portfolios.

**LOE 2.2:** : Increase Army's purchasing power by consolidating enterprise digital requirements

The Army's purchasing power is currently underutilized because of the decentralized approach to procuring IT software, hardware, and services. Industry data shows significant cost savings through strategic sourcing efforts that the Army must fully implement. The Army will achieve this by establishing a category management approach that is complemented by strategic sourcing. These initiatives will increase Army's purchasing power, reducing costs and allowing the Army to redirect savings to other mission priorities. The Army will scale the category management efforts established in FY21 to find additional opportunities for consolidation of requirements across the Commands. Category management will also be utilized to establish standard levels of service for IT support. Granular data on contract execution will be sourced through Computer Hardware, Enterprise Software, and Solutions (CHESS) contracts to provide additional insights into spending and identify opportunities for category management, as well as benchmark outcomes against industry standards. The Army will establish Enterprise License Agreements (ELA) with strategic vendors to both achieve cost savings and reduce procurement manpower through a single contract, as well as drive accountability for the use of licenses by the Commands. The Army must aim to fully determine the usage of procured software and whether the Army is overpaying vendors for unused licenses. The Army will implement a Software Asset Management (SAM) tool to inventory all software on Army enterprise and tactical networks, achieve efficiencies through license distribution, and identify opportunities for new ELAs based on usage patterns.

**LOE 2.3:** Drive audit readiness and remediation

The Army should achieve a clean Working Capital Fund (WCF) and General Fund (GF) audit opinions. To accomplish that objective, the Army must remediate all Notice of Findings and Recommendations (NFR) related to IT General Controls (ITGC) which represent a large percentage of all unremediated NFRs to date. Currently, the Army leads the DoD services in progress made to remediate the findings through Corrective Action Plans (CAPs). The Army must prioritize financial auditability requirements through ITGC in new capabilities such as EBS-C to ensure financial data is processed, stored, and shared completely and accurately. The Army will implement the tools needed to address access control and segregation of duties through an ICAM system since the greatest number of NFRs relate to this requirement. Financial system owners will prioritize integration of their systems to ICAM and establish the required policies and procedures to address both access controls and segregation of duties. The Army will prioritize the implementation of CAPs for Internal Use Software (IUS) by capturing the costs associated with development, fielding and operation, and maintenance at granular levels in the acquisition process leveraging the TBM framework. These efforts will increase business resiliency and technology security for the digital Army while at the same time supporting Army's goal of achieving a Congressionally-mandated clean audit opinion for the Department.

**LOE 2.4:** Increase IT investment accountability by establishing robust financial analytics and governance

The Army must employ strong fiscal stewardship of its IT and Cyber Activities budget to improve business outcomes and increase mission value. The Army will pursue full traceability and oversight of the execution of the digital resources by Commands by improving data access and quality from contracting and acquisition systems. The IT Investment Accountability (ITIA) effort will increase the ability of the Army to see, assess, redirect, and control IT resources. The Army Digital Oversight Council (ADOC) was established in FY21 to help synchronization, to inform Army requirements and resourcing prioritization, and to help technical integration of digital transformation efforts across the Army. The Army will fully leverage the ADOC as a governance forum to manage the digital equities in the PPBE process, including escalation of issues to the IT Oversight Council (ITOC) as needed for decision making by Army Senior Leaders. The Army will continue to expand and scale the use of analytics to identify potential risks and issues in execution of the digital investments. The Army will also reassess and establish new metrics and measures through the current IT Investment Accountability Reform to ensure that the digital investments are meeting mission outcomes.

*"In the face of determined adversaries and accelerating technological advances, we must transform today to meet tomorrow's challenges."*

**—General James C. McConville, Chief of Staff of the Army**

## PEOPLE & PARTNERSHIPS

**OBJECTIVE 3:**

***A tech savvy, operationally effective digital workforce partnered with a robust network of allies, industry, and academia***

People drive success. The Army's people and its relationships with allied partners are vital to achieving the goal to dominate in MDO. In today's digital transformation revolution, simply having the newest technology is not sufficient – the Army needs the right digital skills to optimize, adapt, and fully apply the technology through innovation. Similarly, simply having strong partner relationships is not enough – the Army needs proper channels, networks, and systems in place to effectively collaborate and communicate. The Army workforce must understand, develop, apply, and enable digital priorities as well as external opportunities to improve collaboration with allies, academia, and industry.

The goal is to embrace the recognition that people drive Army's success on and off the battlefield. Robust recruiting and selection, training programs, digital career models, and partnerships with academia and industry will build a digital ready, adaptive, and innovative workforce, with the full range of required digital skills. In addition, sustained communications and interoperability with allied nations will ensure the Army optimizes its ability to collaborate in all domains. The following LOEs will drive the Army's ability to achieve its desired end state as a digital workforce with a network of valuable partners.

**LOE 3.1:** Build and deploy an organic digital workforce with mission critical skillsets by establishing partnerships with industry and academia

The Army workforce must acquire the necessary skillsets to effectively embrace and apply digital technology. The Army has initiated a number of pathfinders and initiatives to address how the Army will hire, retain, train, and deploy the digital workforce of the future. The Army must scale and expand the scope of each pathfinder. The Army will establish a single integrated total Army approach to establish the digital workforce of the future through innovative talent models. The Army will continue to expand and scale pioneering talent management models like the Software Factory. In job postings for technical roles, the Army should include specific skills that applicants will need. The Army will also adopt modern techniques like code reviews to ensure that candidates are properly qualified for their roles. The Army will implement new authorities available such as the Cyber Excepted Service (CES) to hire and retain the best cyber talent on par with the commercial industry.

The Army will continue to develop and implement new concepts and prototypes for acquiring, developing, certifying, and deploying critical skills in AI, data science, cyber, and emerging technology areas. The Army will seek opportunities through its partnerships with academia and industry for rotational programs that enable the Army workforce to gain skills from the partner organization, while also enabling partner organizations to rotate through the Army and coach the workforce. The Army will also better target its recruitment of top talent from its partner organizations. These partnerships will enable the Army to develop a more fully capable workforce that can execute its digital priorities. The Army will also explore and implement innovative employment models for the total workforce, targeted recruitment, and other talent management approaches to bringing top talent into the Army.

**LOE 3.2:** Identify and cultivate the skills needed by the Army of 2028 by fostering digital innovation and continuous learning

The Army must identify and cultivate necessary skills by fostering innovation and continuous learning in order for the workforce to keep pace with changing technology. The Army must establish training for both civilians and military beyond traditional IT and include how digital technologies can be adopted, implemented, and adapted across the Army thereby leading to heavy contractor reliance. The Army must establish robust recruitment and selection, training programs, development opportunities, new workforce models, and strategies to attract, develop, and retain top talent. These efforts will improve the agility and readiness of the digital workforce. The Army will continue to scale the Quantum Leap initiative to reskill and upskill the digital workforce by assessing their skills and abilities and establishing career paths and associated training for career progression. In order to retain the workforce, the Army will establish initiatives to provide hands-on digital experience to the workforce through hackathons, low code/no code programming, and Robotic Process Automation (RPA). The Army will develop a comprehensive Integrated Development Environment to ensure unit-developed solutions are consistent with Army development, data, security, and other standards and are sustainable and expansible as necessary. As the Army develops robust talent, it will carefully track the skills its workforce has developed so it can match them to the best possible roles. New incentives, such as rewards and recognition programs, will be established to motivate the workforce to identify innovation opportunities and for excellence in service delivery. The Army will seek new authorities to more fully employ the digital talent across the active, reserve, and civilian components of the workforce to support any project in the Army at the time of need. New collaboration platforms for crowdsourcing will enable the remote workforce in concert with these new authorities to execute digital projects across the Army based on their skillsets so they are not limited to opportunities within their unit. The Army will utilize communities of interest to connect its digital workforce and facilitate technical discussions

## PEOPLE & PARTNERSHIPS

**LOE 3.3:** Facilitate collaboration with allied partners by strengthening communication and interoperability of data, software, and systems

The success of Joint All Domain Operations depends on the Army's ability to collaborate and coordinate with its allied nation partners. The Army needs to continually improve communication and collaboration with its allied partners, especially with the Five Eye partners and NATO allies. The Army can achieve this by prioritizing the implementation of a modern cloud-based Mission Partner Environment (MPE). MPE will provide the necessary integration, through modern virtual technologies, to enable the interoperability of multinational operations and information sharing across multiple classification levels and protected through a robust ICAM system, with a robust, mission-based Need-to-Know requirement. The Army will also continue to support and work with international standards bodies to establish joint interoperability standards and architecture for JADC2. The Army will reenergize its partnerships with allied nations to leverage and share lessons learned on their digital transformation efforts. The Army will continue to expand and scale tours of duty for personnel from allied nations to the Army and vice-versa.


*Going digital is a mindset, it's culture change… it's about how we can fundamentally change how we operate as an Army through transformative digital technologies, empowering our workforce, and re-engineering our rigid institutional processes to be more agile…"*

**—Dr. Raj Iyer, CIO, U.S. Army**

## FOLLOW THE CIO ONLINE

www.army.mil/CIO

www.facebook.com/ArmyCIO

@ArmyCIO

Army Chief Information Officer