Logistics Information Technology Strategy

Deputy Assistant Secretary of Defense (Logistics)

2024—2029

Message from Deputy Assistant Secretary of Defense for Logistics

It gives me great pleasure to codify the Department of Defense (DoD) modernization and rationalization effort into this Logistics Information Technology (Log IT) Strategy. Improving Log IT systems will enhance the Department's ability to fight and win wars as a superior military force in an era of great power competition, enabling operators and military decision-makers to harness data; driving interoperability and compliance; improving accountability; and leveraging strategic, operational, and tactical opportunities. To date, the Military Services, Defense Agencies, and Field Activities have made significant progress in modernizing and rationalizing our Log IT systems in the DoD Ecosystem. I am very excited to be part of this journey that will span the coming years and look forward to what we will continue to accomplish in this transformational effort.

The Department acknowledges the great achievements and significant efforts of the DoD Component Log IT owners to reach this point. We still have more to accomplish as we embark on an enterprise Log IT Portfolio Management approach to better assess the business health of our systems and reduce technical debt while providing secure systems and new technology to the Warfighter. The Log IT portfolio management strategy improves visibility of the business functions of IT and elevates performance through the effective use of resources, people, funding, assets, and processes maximizing Warfighter capabilities.

Each DoD Component has contributed to the successful reduction of over 90 IT systems from the portfolio since the start of Fiscal Year (FY) 2020. Until recently, modernizing systems and IT applications remained unmanageable due to the lack of the right tools and analytical advancements. This strategy represents a new opportunity for deliberate evaluation, investment, and risk management in the Department. The approach brings together the enterprise elements important to Log IT while working with the Log IT Portfolio Management Offices to develop robust, critical metrics to better assess the business health of our IT systems and the capabilities they need to provide critical data in a contested environment.

The end state of the Log IT Strategy continues the rationalization pathway to reduce the portfolio from more than 400 systems to less than 170 by FY 2029. For years, the Department has accepted risk in Log IT management. Now, through advances in technology, we support a new approach towards how we invest in IT solutions to meet our mission capabilities, reduce IT debt, and deliver superior enterprise logistics.

I remain committed to working with our leaders to implement this strategy and joining together across the entire Department to ensure we are capable and ready to overcome any challenge now and in the future. This Log IT Strategy helps the Department modernize how systems harness data to strengthen our supply chain for the future, improve interoperability and audibility, increase resilience across the enterprise and bring greater capability to the Warfighters, wherever they are and at the time of need.

Leigh E. Method, SES
Deputy Assistant Secretary of Defense for Logistics

Table of Contents

1. Introduction

The Department of Defense (DoD) mission provides the military with the forces needed to deter war and ensure our nation's security. DoD must properly manage and operationalize data as a strategic asset to support a lethal and effective Joint Force that, in collaboration with our network of Allies and Partner Nations, sustains American influence and advances shared security and prosperity.

The Logistics Information Technology (Log IT) portfolio exists in a contested environment and must function across all five warfighting domains: land, sea, air, space, and cyber. This challenge is particularly relevant to denied, degraded, intermittent, or limited communications environments. Every effort to protect logistics data while leveraging quality, interoperability, and advanced technologies, enables rapid decision-making and timely execution. Log IT is critical to logistics command and control and must be designed with both warfighting and business efficiency in mind. Modern wars can be fought on the battlefield through conventional kinetic effects or silently through data and software exploitation. Logistic data is an unrealized weapon and critical vulnerability in its current state. Reliable and accurate data informs leaders of the status of critical assets and empowers operational decisions; poor and unreliable data only benefits our adversaries. Accurate logistics data helps us maintain strategic advantage while inaccurate data causes confusion and disrupts the decision process.

Improving Log IT will enhance the Department's ability to fight and win wars as a superior military force in an era of great power competition, enabling operators and military decision-makers to harness untapped data, leveraging strategic, operational, and tactical opportunities. We have a responsibility to leverage DoD capabilities and investments, thereby earning the trust of the operational Warfighter, the U.S. Congress, and the American people. We must continuously focus on the logistics business processes and utilize enterprise resources for more efficient military operations through logistics. The ability to fully understand the Defense supply chain using a system-of-systems approach is necessary. An effective Log IT network is critical to leverage the full range of capabilities among DoD, U.S. Government Agencies, industry partners, Allies, and Partner Nations. No current solution fully illuminates the entirety of our broad, and complex, supply chain ecosystem. In the future, Combatant Commanders, and logistics planners will leverage the Advanced Analytics (Advana) platform.

The Department continuously adopts new technologies as part of its Digital Modernization program. However, the success of these efforts depends on secure digital infrastructure that considers the complexities of data from external sources, DoD systems, and connected platforms. Adversaries are also in competition to amass data superiority. Whichever side leverages data better will gain military advantage. Our ability to fight and win wars requires that we become world leaders in operationalizing and protecting our data resources at speed and scale.

The Log IT Strategy addresses gaps and challenges caused by divergent priorities and raises awareness of Log IT requirements. It provides clear priorities, goals, objectives, and metrics for leadership and portfolio managers to assess the health of the Log IT portfolio. This effort will move the Department toward a more data-centric environment and increase the reliability of Logistics data across the enterprise.

The Log IT Strategy supports Digital Modernization through the overarching vision, priorities, and objectives necessary to support a data-centric enterprise. While opportunities to improve proficiency and efficiency are everywhere, this strategy focuses on policy compliance, data analytics, audit, and portfolio rationalization. Success cannot be taken for granted. These goals provide context and direction for each DoD Component, Executive Agent, and other responsible organizations to develop or update their own strategic plans, process innovations, and investments. We must treat data as a weapon system, identifying any critical vulnerabilities while optimizing, securing, and using the data for operational effect.

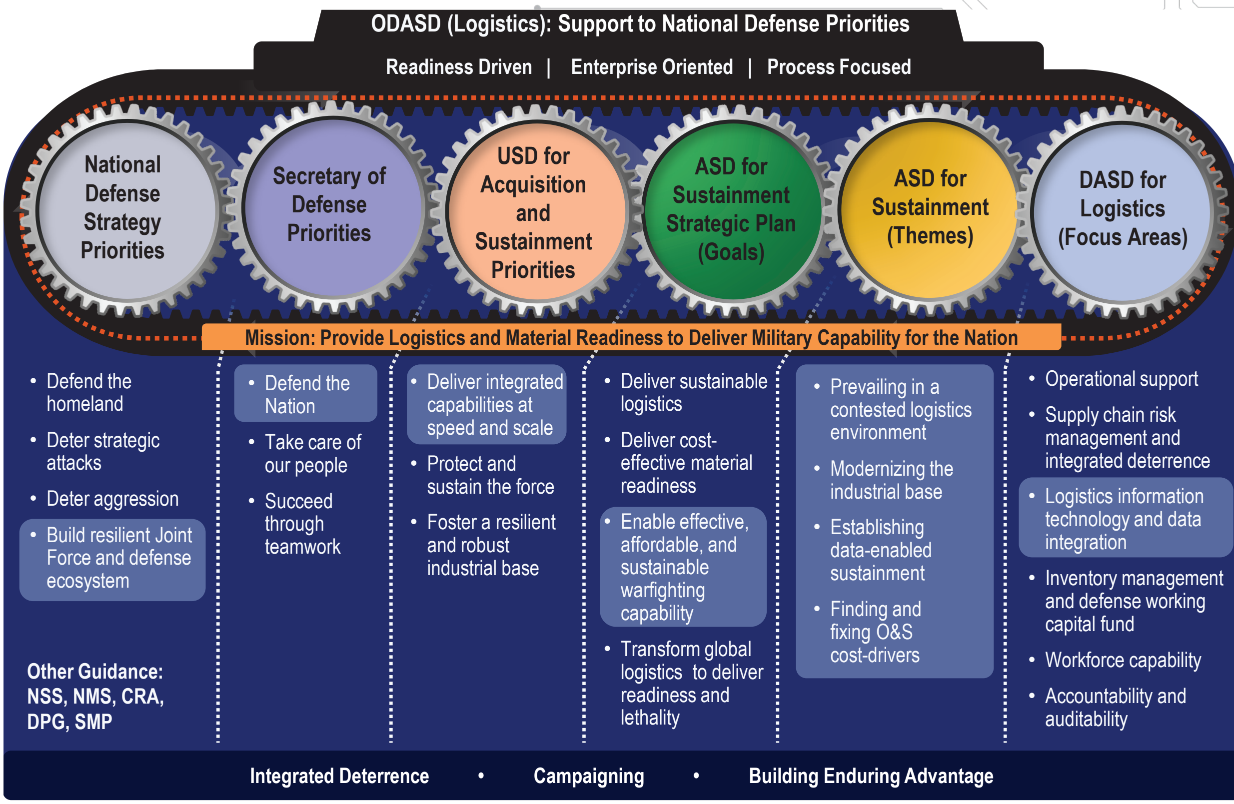

Figure 1: Alignment to Strategic Priorities and Objectives.

The chart highlights the areas where the Log IT Strategy supports DoD strategic priorities, goals, themes, and focus areas. Acronyms for Figure 1 are defined in the "Acronym and Abbreviation List."

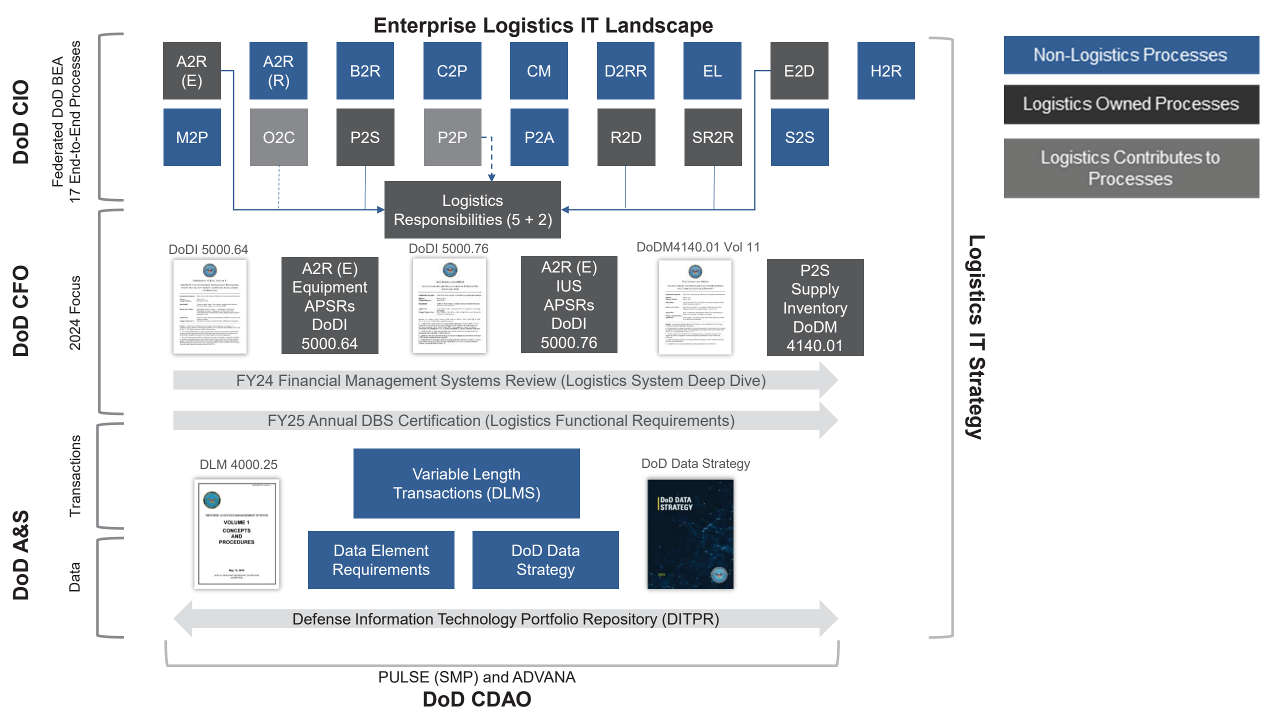

Figure 2: Enterprise Logistics IT Landscape.

The Logistics IT Strategy integrates requirements from across DoD: from the Federated Business Enterprise Architecture (BEA) level to the transactional level to individual data elements. It also accounts for DoD efforts supporting Defense Business System (DBS) certification and the Financial Management Systems Review.

1.1. Problem Statement

Today, the Department lacks an integrated, enterprise strategy for Log IT modernization. This deficiency has created divergent priorities throughout the Joint Force, Defense Agencies, Field Activities, Allies, and Partner Nations for investment and system requirements, diminished effectiveness, and continued unmitigated audit material weaknesses. Logistics IT has fallen behind emergent and evolving IT constructs, creating operational- and tactical-level divergence of effort and focus. Improved Log IT will enable the Department to fight and win in an era of great power competition. It will empower operators and military decision-makers to harness data and leverage strategic, operational, and tactical opportunities in ways not possible today. This document develops a Departmental Log IT strategy for modernization in conjunction with the DoD Components and establishes performance targets for Log IT systems in partnership with the DoD Chief Information Officer (CIO), Chief Digital and Artificial Intelligence Officer (CDAO), and Chief Financial Officer (CFO) to enable compliance with policy and achievement of auditability requirements. The Department lacks the proper unifying tools to effectively trace capabilities to requirements, requirements to specifications, specifications to allocation, and allocation to enablers. Continued work on integrating enterprise architecture and modernization is underway to incorporate other Log IT systems, addressing that capability shortfall.

1.2. Scope

The Log IT Strategy applies to the entire DoD portfolio of information technology systems that conduct logistics functions, such as supply, transportation, maintenance, property accountability functions, and business processes for fiscal years (FY) 2024 to 2029. This strategy also recognizes and includes those IT systems where the Deputy Assistant Secretary of Defense for Logistics (DASD(Log)) is the Office of the Secretary of Defense (OSD) proponent, functional requirements owner, primary OSD advocate, or has principal equities in the system's lifecycle. [1]

[1] DASD(Log) is the functional proponent for the Defense Property Accountability System, Synchronized Predeployment and Operational Tracker-Enterprise Suite, and Joint Transportation Management System.

2. Background

The Government Accountability Office (GAO) assessed the Department's DBS as a "high risk area" (GAO-20-253).[2] Log IT systems include a significant portion of the Department's DBS portfolio, national security systems, and financial feeder systems as they pertain to logistics functions. DoD continues to emphasize auditability as a critical enabler to efficient operations and mission success. In addition, the DoD Strategic Management Plan includes a performance goal to "Provide Effective Logistics Information Technology" in support of Departmental strategic priorities and objectives.[3]

The Joint Concept for Contested Logistics (JCCL) is one of the four Joint Warfighting supporting concepts that seeks to achieve agile and resilient logistics. The JCCL attributes of responsiveness, simplicity, flexibility, economy, attainability, sustainability, survivability, and visibility (situational awareness) support integrated operations across the Joint Logistics Enterprise. To retain the strategic comparative advantage to globally posture, deploy, employ, and sustain forces, the Department must invest in Log IT to improve decision-making and operational support.

The Assistant Secretary of Defense for Sustainment (ASD(S)) Strategic Plan highlights DoD's journey to expand and optimize logistics data integration and the need to develop logistics enhancements and improve mission enablers (ASD(S) Strategic Plan Objective 1.3). Furthermore, the ASD(S) Strategic Plan directs modernization of Component Log IT systems and the improvement of data analytics (ASD(S) Strategic Plan Line of Effort 1.3.3.).[4]

The DoD CIO published the DoD Data Strategy in 2020, clearly laying out the central goals for data as visible, accessible, understandable, linked, trustworthy, interoperable, and secure. These tenets are commonly referred to as the "VAULTIS" goals. This Log IT Strategy supports the path to achieving VAULTIS compliance through the timely implementation of the interoperable data and interface protocols as detailed in the Defense Logistics Management Standards (DLMS).[5]

The DLMS provide the templates for electronic data interchange (EDI) for the systems that underpin core business processes of the global logistics and supply chain management enterprise. The current DoD BEA designates DLMS as the enterprise standard for logistics systems. DLMS enables accurate transactions for logistics operations and promotes interoperability between DoD activities and external trading partners. DoD Manual (DoDM) 4140.01, Volume 8, directs DoD Components to implement DLMS to ensure interoperability among the functional areas of supply, transportation, contract administration, pipeline measurement, physical inventory control, and finance.[6] The Defense Logistics Manual (DLM) 4000.25 specifies DLMS compliance requirements.[7] By implementing interoperability and data standards, the Department establishes a data-informed sustainment environment and uses data analytics platforms to illuminate the global supply chain. The ability to send and receive variable-length transactions is central to promoting interoperability, flexibility, and data quality.

Existing policies reflect required data elements for Log IT systems. DoD Instruction (DoDI) 5000.64 and DoDI 5000.76 establish required data elements for Accountable Property Systems of Record (APSR) for equipment and internal use software, respectively.[8] DoDM 4140.01, Volume 11, establishes required data elements for inventory and materiel management Log IT systems.[9] Compliance with these requirements supports logistics data analytics, total asset visibility, and auditability. These data elements are foundational, along with variable-length transaction capability, to align business processes with policy and implement DLMS to promote interoperability throughout the logistics environment.

---

[2] GAO-20-253, "Business Systems Modernization," March 5, 2020.
[3] DoD Strategic Management Plan, Fiscal Years 2022–2026.
[4] Assistant Secretary of Defense for Sustainment Strategic Plan, Fiscal Years 2023-2029, October 2022.
[5] DoD Data Strategy, September 30, 2020.
[6] DoDM 4140.01 Vol 8, "DoD Supply Chain Materiel Management Procedures: Materiel Data Management and Exchange," February 10, 2014, as amended.
[7] DLM 4000.25, "Defense Logistics Management Standards (DLMS)," date varies by volume.
[8] DoDI 5000.64, "Accountability and Management of DoD Equipment and Other Accountable Property," June 10, 2019; DoDI 5000.76, "Accountability and Management of Internal Use Software (IUS)," June 7, 2019.
[9] DoDM 4140.01, Volume 11, "DoD Supply Chain Materiel Management Procedures: Inventory Accountability and Special Management and Handling," March 8, 2017.

The Defense Transportation Electronic Board (DTEB) is responsible for the DoD standard for X12 EDI among the Log IT systems that perform transportation functions. The United States Transportation Command (USTRANSCOM) chairs the DTEB Committee for synchronizing and implementing 36 standard exchanges applied by 14 systems across the Joint Deployment and Distribution Enterprise (JDDE).

The DTEB enables standardized data exchange between DoD components, systems, and commercial trading partners and ensures compliance with the American National Standards Institute (ANSI) Accredited Standards Committee X12 standard for EDI as directed by Department of Defense Directive (DoDD) 8190.01E (DLMS). Standards maintained and developed by the DTEB span processes across the entire Defense Transportation System and are prescribed in the Defense Transportation Regulation.

The Log IT Strategy's mission and vision statements provide a way ahead at the right cost, with improved capabilities to the Warfighter, and modern technologies for the Department.

3. Mission Statement

Drive warfighting readiness and lethality through efficient and effective operation and improvement of the Joint Logistics Enterprise through Log IT and data-informed decisions.

4. Vision Statement

A secure and interoperable logistics information environment that uses accurate and trusted data at speed and scale for operational advantage, enhanced responsiveness, business productivity across DoD, the Joint Logistics Enterprise, and the Total Force for the full range of operational environments.

5. Strategy

5.1. Priorities for Focus Areas

- Data quality
- Audit compliance and Financial Improvement and Audit Remediation (FIAR)
- Interoperability and standardization
- Automated and modernized Log IT systems
- Predictive forecasting of investments for system requirements and changes
- Achievement of the Warfighter's requirement with minimal Log IT costs

5.2. Goals and Enabling Objectives

5.2.1. Goal 1: Optimize the Log IT Systems Environment

Log IT systems must comply with the Department's functional requirements to improve reconciliations between property systems for improved data quality and auditability. Log IT systems must also continue operating in degraded, disconnected, intermittent, and limited (bandwidth) environments for an extended period to enable resilient and flexible logistics, as appropriate.

Objective 1.1. Compliance for auditability and asset visibility. DoD must meet many regulations and standards to maintain compliance and audit readiness, including Service Organization Control 1 (SOC 1), as applicable. Core Log IT systems must comply with policy and audit requirements, including DLMS (DoDD 8190.01E, DoDM 4140.01 Volume 8, and DLM 4000.25), accountability requirements (DoDI 5000.64, DoDI 5000.76, and DoDM 4140.01 V11), and DTEB EDIs. Audit readiness is military readiness and integrated deterrence.

Objective 1.1.1. Designate the Component lead or representative responsible for periodic reporting and status tracking of implementation plans for DLMS, DTEB, and policy compliance.

Objective 1.1.2. Identify funding shortfalls and requirements to implement DLMS and DTEB policy compliance by Component.

Objective 1.1.3. Identify critical logistics system attributes and incorporate into authoritative data sources.

Performance Metrics[10]

Metric 1.1. Total number of Log IT systems in the portfolio

Metric 1.2. Number of core Log IT systems compliant with DoDI 5000.64

Metric 1.3. Number of core Log IT systems compliant with DoDI 5000.76

Metric 1.4. Number of core Log IT systems compliant with DoDM 4140.01, Volume 11

Metric 1.5. Number of core Log IT systems capable of variable-length transactions

Metric 1.6. Number of Approved DLMS Changes (ADC) implemented

Metric 1.7. Number of Log IT system compliant with DLMS in accordance with DLM 4000.25

Metric 1.8. Number of core Log IT systems compliant with DTEB EDIs

[10] Specific measures, thresholds, and operationalization of metrics are in development and will be published separately. Current metrics reflect critical aspects of Log IT to assess to gauge progress against the Logistics IT Strategy.

Metric 1.9. Number of DTEB Data Management changes implemented

Metric 1.10. Multiple Component System Use: Number of SOC 1–reportable core Log IT system

Metric 1.11. Number of Internal Controls Over Financial Reporting relevant systems, and number of legacy IT systems waived based on the annual Financial Management Systems Review

5.2.2. Goal 2: Promote Data Visibility and Quality

Data is critical to decision-making and business operations for DoD. Focusing on data increases analytics capabilities and reduces discrete and redundant data lakes, data warehouses, dashboards, and business analytics tools. Developing automation reduces the chance of human error and increases data accuracy. The logistics community will leverage Advana, the Department's primary enterprise authoritative data management and analytics platform for informed decision-making.[11]

To promote logistics data as a trusted resource for leaders, data must be accurate, standardized, and accessible. .

Objective 2.1. Availability of system data in authoritative sources. The program management system data and metadata in authoritative sources, such as the DoD Information Technology Portfolio Repository (DITPR), Defense Information Technology Investment Portal (DITIP), and the Select and Native Programing Data Input System for Information Technology (SNaP-IT) are critical for gaining insight into the Log IT portfolio. In addition, Log IT systems must work to meet the VAULTIS goals established in the DoD Data Strategy to support and improve DoD as a data-centric organization.

Objective 2.2. Use data analytics platforms to accelerate decision-making. The Log IT community shall use DoD authoritative sources to visualize data, breakdown information silos, and more rapidly identify critical data and data quality issues.

Objective 2.3. Improve DLMS data management to meet the DoD Data Strategy. Data standards alone cannot improve data quality, they must be continuously informed by feedback from policy management bodies (DTEB, DLMS Process Review Committee, etc.) and users who consume, produce, manage, and govern data, with particular emphasis on focus areas of the logistics community.

Objective 2.4. Improve overall data integrity to meet the DoD Data Strategy. The availability and quality of system production data across the Department portfolios provides visibility of logistics activities and moves the Department closer to being a data-centric organization. Integrating the data elements in the production environment further refines confidence in the reliability of data for compliance standards and appropriate financial investments.

Performance Metrics

Metric 2.1. Data availability in authoritative sources (DITPR, SNaP-IT, and DITIP)

Metric 2.2. Number of Log IT systems providing data in Advana

Metric 2.3. Number of Log IT system-related Notices of Findings and Recommendations, and status by Component

Metric 2.4. Percentage of Log IT systems compliant with Logistics Functional Requirements (policy compliance, DLMS, DoDI 5000.64, and DoDM 4140.01 Volume 11)

[11] FY2018 National Defense Authorization Act, Section 911-913; Advana is the DoD's enterprise-wide, multi-domain data, analytics, and artificial intelligence (AI) platform that provides military and civilian decision makers, analysts, and builders with unprecedented access to enterprise tools and capabilities—all in a scalable, reliable, and secure environment. Advana is a platform that offers tools to perform data exploration, analysis, model development, data visualization, and more. In addition, Advana hosts hundreds of curated applications providing analytics for over a dozen lines of business—including logistics—available for DoD customers everywhere to leverage. Using one central platform with right-time data, tools, and other self-service products, Advana puts the power of data, analytics, and AI in the pocket of every analyst and decision-making authority at the DoD.

5.2.3. Goal 3: Right-Size the Log IT Portfolio

Retire legacy systems and accelerate optimization of modern enterprise solutions by collaborating with all stakeholders across end-to-end business processes, leveraging proven capabilities, and achieving system commonality. Legacy systems are costly, create cyber risk, and impede auditability. Portfolio management identifies redundant systems for sunsetting, with a focus on systems not compliant with policy and audit requirements. Retiring outdated systems and investing in audit-readiness accelerates compliance. DoD Components must also consider the range of existing Log IT solutions across the enterprise before investing in new capabilities or systems. Using projections briefed to the Logistics Executive Steering Committee (LESC) in August 2023, the Log IT portfolio is expected to reduce from over 400 systems in FY23 to less than 170 by the end of FY29.

	FY23	FY24	FY25	FY26	FY27	FY28	FY29
Total Portfolio Systems	433	384	340	301	241	203	166

Table 1: The Log IT System Portfolio Transition Plan from FY23 through FY29.

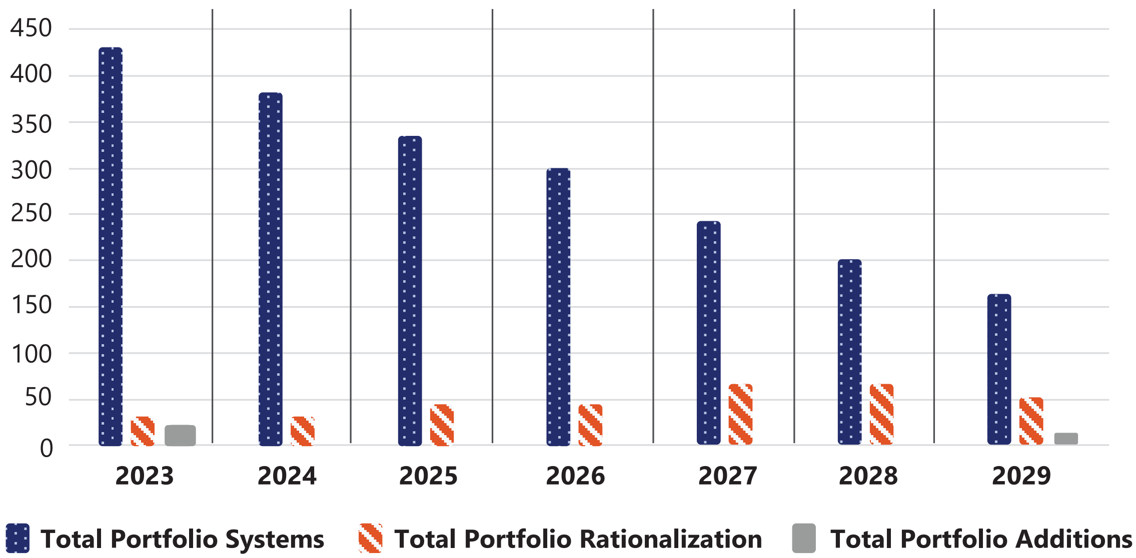

Figure 3: Projected Log IT portfolio (DBS) Reduction.
Note: The figure is based on the Component briefings to the Logistics Executive Steering Committee August 9–10, 2023.

To enable, highlight, and realize opportunities for rationalization, the Department needs to view system capabilities and compliance measures across the enterprise using authoritative data sources.

Objective 3.1. Identify redundant functionality and optimization opportunities beyond DoD CIO-covered and priority systems. Aligning systems to the DoD BEA processes and operational activities illuminates opportunities to consolidate systems and improve efficiency in the Log IT portfolio.

Objective 3.2. Identify redundant capabilities across logistics systems (DBS and non-DBS). Developing mechanisms to regularly evaluate capabilities and logistics processes across mission areas supports optimization of systems required to assert to the BEA.

Objective 3.3. Reduce overall sustainment costs. Retiring legacy systems, consolidating redundant systems, and reinvesting in modern capabilities and existing compliant systems avoids unnecessary maintenance costs and protects against cyber risk.

Performance Metrics

Metric 3.1. Number of Log IT systems retired annually and planned for retirement over the Future Years Defense Program

Metric 3.2. Annually report Log IT sustainment costs

Metric 3.3. Percentage of systems in each quadrant of the OSD CIO Quad tool analysis

5.2.4. Goal 4: Modernize and Secure Log IT Systems

Digital innovation is changing the way the modern world produces and consumes information and how emergent business systems operate. With adversaries seeking to exploit vulnerabilities, modernization is critical to protecting our systems and data. Implementing the seven pillars of the DoD's Zero Trust framework across the DoD information enterprise serves to protect network infrastructure, services, systems, and embedded communication platforms. Zero Trust is a robust cybersecurity model that eliminates the idea of trusted or untrusted networks, devices, personas, or processes and shifts to multi-attribute-based confidence levels to enable authentication and authorization policies based on the concept of least privileged access. This goal and supporting objectives align to DoD CIO's strategic plan and DBS guidance from Section 2222 of Title 10, United States Code (U.S.C.).[12]

Objective 4.1. Implement Identity, Credential, and Access Management (ICAM) solutions. In support of the DoD Zero Trust Architecture (ZTA), implement the ICAM Strategy and capabilities published by the DoD CIO for all DoD information systems, including Log IT systems. ICAM simplifies user authentication and streamlines account creation while providing a more secure information environment. Additional microservice design of application and data operations further enhances the ZTA implementation.

Objective 4.2. Migrate Log IT systems to the cloud. DoD has siloed IT systems distributed across modern and legacy infrastructure around the globe, leading to issues impacting the ability to organize, analyze, secure, scale, and capitalize on critical information for timely, data-driven decisions. Cloud-based network storage enables users to access information from anywhere at any time. The Log IT community must take full advantage of this enabler, acknowledging that not all systems can or will migrate to the cloud.

Performance Metrics

Metric 4.1. Number of ICAM-compliant Log IT systems (DoD CIO-led metric)

Metric 4.2. Number of Log IT systems migrated to and operating in the cloud (DoD CIO-led metric)

[12] "Fiscal Year 2024 Defense Business Systems Annual Certification Guidance" Memorandum, July 31, 2023; "Identity, Credential, and Access Management (ICAM) Strategy," March 30, 2020.

5.2.5. Goal 5: Program Objective Memorandum (POM) Funding for Investment Decisions

Sustaining the Department's Log IT portfolio equates to $2.2 billion, approximately 27% of the DoD DBS portfolio budget in FY24, and represents 39% of the enduring DoD audit systems. In addition, the Log IT business mission area consists of over 400 systems and represents the largest category of active systems in the Department's DBS portfolio. This portfolio accounts for over $800 billion in DoD assets. The quantity of systems represents a high risk to auditability, interoperability, and modernization. Proactive monitoring, review, and submission of Program and Budget Review funding requirements for Log IT enables the portfolio to target IT investments supporting the ASD(S) Strategic Plan and Departmental objectives. This goal is based on the services' rationalization plans (Figure 3) for rightsizing resources and improving performance.

Objective 5.1. Valuation of POM Investments. Through analyzing Component and Program Office FY funding profiles against implemented DLMS system changes, transactions, and corrective action plans, the Log IT portfolio can evaluate gaps and resource selected enhancements for funding.

Performance Metrics

Metric 5.1. Number of data-aligned system capabilities appropriately resourced per FY

Metric 5.2. Number of systems capabilities appropriately resourced by value

Metric 5.3. Number and value of unfunded Log IT system upgrades, modifications, modernization, or decommission over the Future Years Defense Program

Metric 5.4. Assessed funding shortfalls in the year of execution

Metric 5.5. Develop a Log IT Portfolio Scorecard to assess overall portfolio business health, leveraging the Log IT Strategy metrics for data-driven decision-making

5.3. Data Interoperability Maturity Model

Data elements are the building blocks of transactions that enable interoperability, accountability, asset visibility, and auditability; all aspects which should be considered as part of implementation plans for this strategy. Available requisite data, joined with variable-length transactions (including DLMS, ANSI X12, XML, and any additional technology adopted by the DoD), business rules, and change management supports the Department's ability to reach the desired Data Interoperability Maturity Model outcomes. The following maturity model (Figure 4) represents a compliance pathway enabling interoperability among DoD Components.

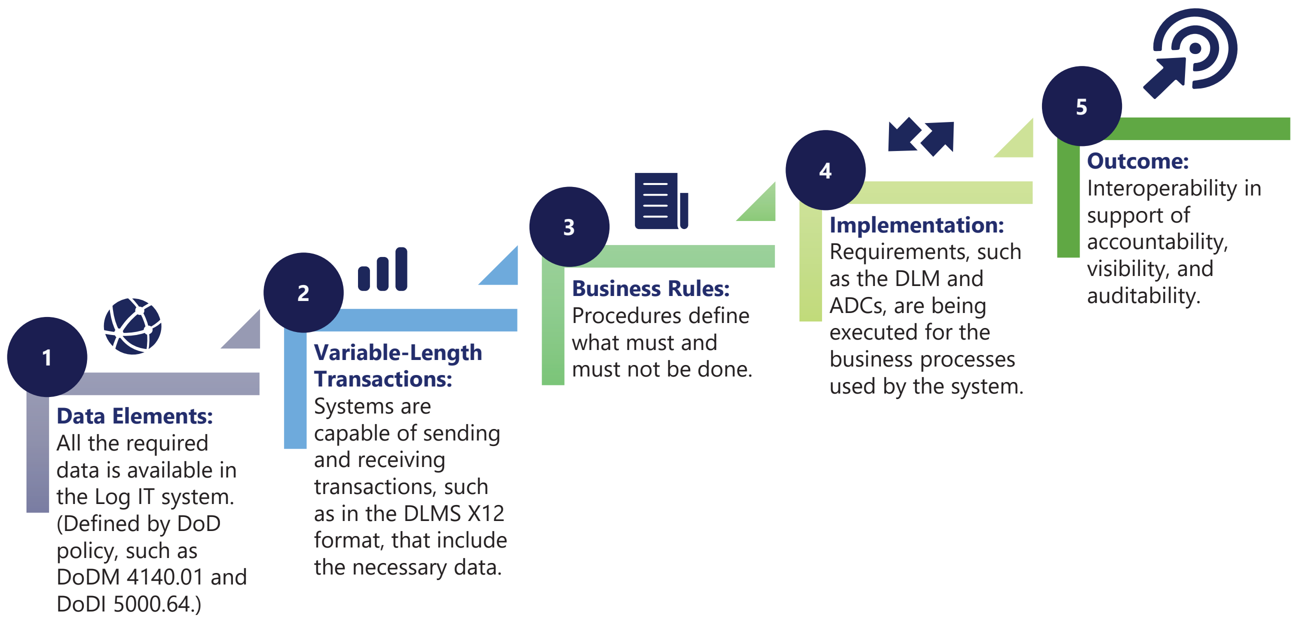

Figure 4: Data Interoperability Maturity Model

5.4. Implementation Plans

The Data Interoperability Maturity Module must be considered when assessing modernization and rationalization plans, since it is the building block for IT system compliance and achieving auditability. To implement this Log IT Strategy, Components will develop or convert their Log IT strategies into measurable Log IT Strategy Implementation Plans. The Component's designated Log IT Portfolio Management Office will report on and monitor implementation. This information will be used to identify milestones, track progress, and illustrate improvements for stakeholders. In general, DoD will achieve Log IT transformation efforts by FY29 or through Component plans for measurable progress as identified in this strategy.

5.5. Governance

To manage the implementation of this strategy and provide further direction, as required, various governance forums exist to resolve issues and advocate solutions. The listed governance bodies play a role in overseeing or guiding this strategy.

Deputy's Management Action Group (DMAG): The DMAG is the primary civilian-military management forum that supports the Secretary of Defense and addresses top Departmental issues that have resource, management, and broad strategic or policy implications. The DMAG's primary mission is to advise the Deputy Secretary of Defense (DSD) in a collaborative environment and ensure that the DMAG execution aligns with the Secretary of Defense's priorities as well as the planning and programming schedule. The DMAG is co-chaired by the DSD and Vice Chairman of the Joint Chiefs of Staff, with Secretaries of the Military Departments, Chiefs of the Military Services, and DoD Principal Staff Assistants holding standing invitations.

Defense Business Council (DBC): The DBC is the principal governance body for vetting issues related to management, improvement of defense business operations, and other issues, including performance management, pursuant to the Government Performance and Results Modernization Act of 2010. The DBC serves as the Department's advisory council on developing the defense BEA, reengineering the Department's business processes, developing and deploying DBS, developing requirements for the DBS (pursuant to Section 2222 of Title 10, U.S.C), and reviewing information technology infrastructure investments (pursuant to Section 2223 of Title 10, U.S.C.). The DBC holds the information technology infrastructure investment review board (pursuant to the DoD CIO's responsibilities in Section 2223 of Title 10, U.S.C.) and Section 11315 of Title 40, U.S.C. to ensure interoperability and reduction of IT duplication; alignment of IT infrastructure investments with the Joint Information Enterprise initiative, enterprise architecture and standards; and adherence to cyber security standards.

Financial Improvement and Audit Remediation (FIAR) Governance Board (FGB): The FGB provides vision, leadership, oversight, and accountability for the Department of Defense's effort to achieve and sustain full financial auditability. Logistics IT plays a critical part in auditability and improving financial processes.

Joint Deployment and Distribution Executive Board (JDDEB): The JDDEB forum drives global integration across the JDDE for planning, operations, and posture in support of national security objectives. The JDDEB drives a unified approach to develop cross-functional solutions and associated action plans to resolve JDDE capability gaps and challenges tied to achieving the objectives of the National Defense Strategy and the National Military Strategy. The JDDEB is chaired by the Commander, USTRANSCOM. Members are DASD(Log), Joint Staff J4, Commands and Services, the Director of the Defense Logistics Agency, the Director of the Defense Health Agency, USTRANSCOM Components, and Subordinate Commands.

Property Functional Council (PFC): The PFC serves as the DoD governance and oversight body and decision-making authority for all recommendations impacting Inventory and Related Property (I&RP) and General Property, Plant, and Equipment (GPP&E). The PFC supports the Department's efforts to remediate audit deficiencies, including self-identified gaps, material weaknesses, and the Secretary of Defense priorities related to I&RP and GPP&E to support the DoD mission.

Sustainment Executive Steering Committee (SESC): Recognizing the breath of DoD sustainment, the SESC is a decision body for cross-cutting sustainment policies, programs, and associated activities. The SESC advises the Assistant Secretary of Defense for Sustainment on innovative solutions to systemic sustainment issues. The SESC aligns Department guidance across materiel readiness, product support, lifecycle costs, joint planning, and supply programs. The SESC can broadly undertake weapon system issues but SESC's primary function is to address systemic sustainment challenges. In doing so, the SESC assesses, recommends, and, where appropriate, approves initiatives to address systemic sustainment issues across weapon systems lifecycles and align solutions to inform and shape the Planning, Programming, Budgeting, and Execution process. Recommendations, outcomes, and analysis are incorporated in the Defense Planning Guidance, summer studies, and issue teams.

Logistics Executive Steering Committee (LESC): The LESC is the executive steering group bringing together supply chain stakeholders from across DoD to lead policy and process improvements in DoD logistics to ensure Warfighter readiness by providing the right item, in the right quantity, at the right time, and at the right cost. The LESC provides oversight and direction to strengthen the capabilities of the logistics enterprise, including Logistic IT and DLMS.

Transportation Management Enterprise Council (TMEC): The TMEC provides strategic direction and removes roadblocks to implement an enterprise-wide, commercial off-the-shelf Transportation Management System (TMS); sustain and maintain the central repository for transportation key supporting documents; approve the degree of financial processing performed in conjunction with the TMS for requesting, managing, and controlling transportation funds; and ensure standardized policies, procedures, and business rules are developed for the processing, documenting, and retention of transportation requirements.

Conclusion

Modernizing and improving the Log IT environment is vital to supporting the Warfighter, achieving the mission, improving the Department's audit position, and efficiently using taxpayer resources. We must continue our pursuit of excellence and set high expectations to achieve breakthrough performance. The meaningful changes laid out in this strategy will increase accountability, traceability, accessibility, trust, and the security of logistics data. This is a living document. We will continue to incorporate new efforts underway that impact this Log IT Strategy.

Acronym and Abbreviation List

Acronym or Abbreviation	Full Form
ADC	Approved Defense Logistics Management Standards Change
Advana	Advanced Analytics
AI	Artificial Intelligence
APSR	Accountable Property System of Record
ASD(S)	Assistant Secretary of Defense for Sustainment
BEA	Business Enterprise Architecture
CDAO	Chief Digital and Artificial Intelligence Officer
CFO	Chief Financial Officer
CIO	Chief Information Officer
CRA	Continuing Resolution Act
DASD	Deputy Assistant Secretary of Defense
DBC	Defense Business Council
DBS	Defense Business System
DITIP	Defense Information Technology Investment Portal
DITPR	DoD Information Technology Portfolio Repository
DLM	Defense Logistics Manual
DLMS	Defense Logistics Management Standard
DMAG	Deputy's Management Action Group
DoD	Department of Defense
DoDD	Department of Defense Directive
DoDI	Department of Defense Instruction
DoDM	Department of Defense Manual
DPG	Defense Planning Guidance
DSD	Deputy Secretary of Defense
DTEB	Defense Transportation Electronic Board
DTR	Defense Transportation Regulation
EDI	Electronic data interchange
FGB	Financial Improvement and Audit Remediation Governance Board
FIAR	Financial Improvement and Audit Remediation
FY	Fiscal Year
GAO	Government Accountability Office
GPP&E	General Property, Plant, and Equipment
I&RP	Inventory and Related Property
I&RP	Inventory and Related Property

ICAM	Identity, Credential, and Access Management
IUS	Internal Use Software
JCCL	Joint Concept for Contested Logistics
JDDE	Joint Deployment and Distribution Enterprise
JDDEB	Joint Deployment and Distribution Executive Board
JP	Joint Publication
LESC	Logistics Executive Steering Committee
Log IT	Logistics Information Technology
NDAA	National Defense Authorization Act
NMS	National Military Strategy
NSS	National Security Strategy
O&S	Operating and Support
ODASD	Office of the Deputy Assistant Secretary of Defense
OSD	Office of the Secretary of Defense
PFC	Property Functional Council
POM	Program Objective Memorandum
SESC	Sustainment Executive Steering Committee
SMP	Strategic Management Plan
SNaP-IT	Select and Native Programing Data Input System for Information Technology
SOC	Service Organization Control
TMEC	Transportation Management Enterprise Council
TMS	Transportation Management System
USD	Undersecretary of Defense
USTRANSCOM	United States Transportation Command
VAULTIS	Visible, accessible, understandable, linked, trustworthy, interoperable, and secure
ZTA	Zero Trust Architecture

Glossary

Accountable Property System of Record (APSR): The Government system used to control and manage accountable property records; a subset of existing organizational processes related to the lifecycle management of property; the system that is integrated with the core financial system.

Alliance: The relationship that results from a formal agreement between two or more nations for broad, long-term objectives that further the common interests of the members.

Core System: An enduring system with a sunset date greater than 36 months from the start of the fiscal year. For consistency, core status in DITPR is calculated the same for both covered and non-covered as more than 36 months.

Defense Logistics Management Standards (DLMS): A process governing logistics functional business management standards and practices across DoD. A broad base of business rules, including uniform policies, procedures, time standards, transactions, and data management, to meet DoD requirements for global supply chain management system support. DLMS provides the DoD standards for EDI among the automated information systems of the DoD supply chain management system.

Identity, Credential, and Access Management (ICAM): The full range of activities related to the creation of digital identities and maintenance of associated attributes, credential issuance for person or non-person entities, authentication using the credentials, and making access management control decisions based on authenticated identities and associated attributes.

Internal Use Software (IUS): Software that is acquired or developed to meet the entity's internal or operational needs (intended purpose); a standalone application, or the combined software components of an IT system that can consist of multiple applications, modules, or other software components integrated and used to fulfill the entity's internal or operational needs (software type); used to operate an entity's programs (e.g., financial and administrative software, including for project management); used to produce the entity's goods and provide services (e.g., maintenance work order management, loan servicing); or developed or obtained for internal use and subsequently provided to other federal entities with or without reimbursement. Not software integrated into and necessary to operate property, plant, and equipment rather than perform an application.

Logistics Information Technology (Log IT) Portfolio Scorecard: ODASD(Logistics) will develop a DoD-wide Log IT Portfolio scorecard to drive accountability and oversight of actions stated in this document. The scorecard is envisioned as a standalone oversight tool to be provided periodically to senior management with milestones.

Partner Nation: A nation that the United States works with in a specific situation or operation.

Technical Debt: An element of design or implementation that is expedient in the short term, but that would result in a technical context that can make a future change costlier or impossible.

Find other terms and their definitions in the glossary of DoD supply chain terms and definitions maintained on the Deputy Assistant Secretary of Defense for Logistics website (https://www.acq.osd.mil/log/LOG_SD/policy_vault.html) and the DoD Dictionary of Military and Associated Terms (https://jdeis.js.mil/jdeis/new_pubs/dictionary.pdf).

References

Assistant Secretary of Defense for Sustainment Strategic Plan, Fiscal Years 2023-2029, October 2022.

Defense Business Systems Investment Management Guidance, version 4.1, June 26, 2018.

Defense Transportation Regulation (DTR) 4500.9R.

DoD Cloud Strategy, December 2018.

DoD Data Strategy, September 30, 2020.

DoD Identity, Credential, and Access Management Strategy, March 30, 2020.

DoD Strategic Management Plan, Fiscal Years 2022–2026.

DoDD 4151.18, “Maintenance of Military Materiel,” August 31, 2018.

DoDD 8190.01E, “Defense Logistics Management Standards (DLMS),” December 30, 2019.

DoDI 4140.01, “DoD Supply Chain Materiel Management Policy,” March 6, 2019.

DoDI 5000.64, “Accountability and Management of DoD Equipment and Other Accountable Property,” June 10, 2019.

DoDI 5000.75, “Business Systems Requirements and Acquisition,” January 24, 2020.

DoDI 5000.76, “Accountability and Management of Internal Use Software (IUS),” June 7, 2019.

DoDI 5000.82, “Requirements for the acquisition of Digital Capabilities,” June 1, 2023.

DoDI 8115.02, “Information Technology Portfolio Management Implementation,” October 30, 2006.

DoDM 4140.01 Volume 8, “DoD Supply Chain Materiel Management Procedures: Materiel Data Management and Exchange,” February 10, 2014, as amended.

DoDM 4140.01 Volume 11, “DoD Supply Chain Materiel Management Procedures: Inventory Accountability and Special Management and Handling,” March 8, 2017.

DLM 4000.25, “Defense Logistics Management Standards (DLMS),” date varies by volume.

GAO-20-253, “Business Systems Modernization,” March 5, 2020.

Joint Concept for Logistics, September 25, 2015.

Office of the Chairman of the Joint Chiefs of Staff, “DoD Dictionary of Military and Associated Terms,” current edition.

United States Code, Title 10, Section 2222, “Defense Business Systems,” December 22, 2022.

Deputy Assistant Secretary
of Defense (Logistics)

2024—2029