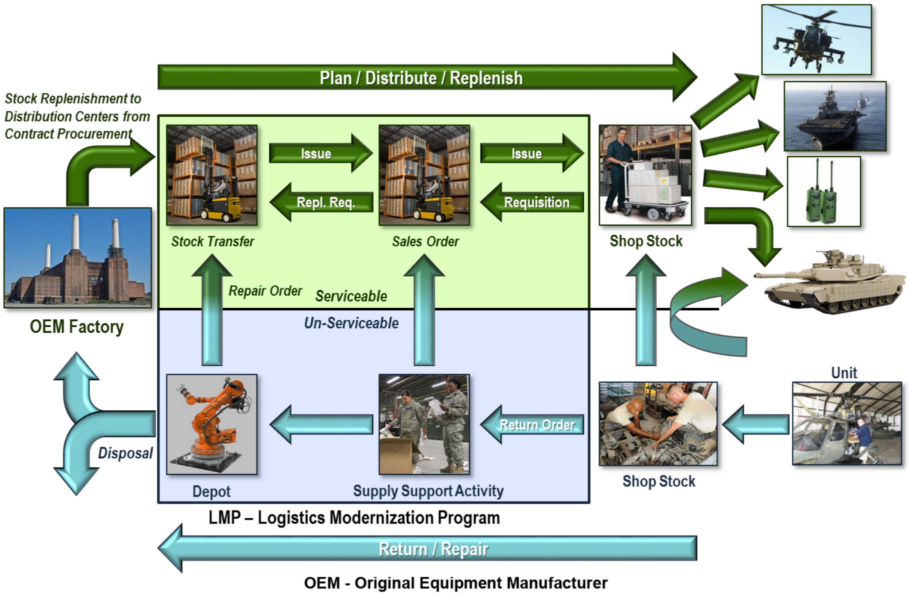
Logistics Modernization Program (LMP)

Executive Summary

- From September 8 through November 20, 2015, the Army Test and Evaluation Command (ATEC) conducted the IOT&E of the Logistics Modernization Program (LMP) Increment 2 Wave 3 Release 7 at three Army Materiel Command (AMC) depots. The test and evaluation of LMP was adequate to support a DOT&E assessment of operational effectiveness, suitability, and survivability.
- LMP is operationally effective. The system successfully completed 98 percent of the observed tasks and successfully processed more than 99 percent of the more than 1.3 million Intermediate Documents to and from interfacing systems in 2015. Since LMP Increment 2 Wave 3 Release 7 went live in June 2015, users reported zero critical or major problems.



- LMP is operationally suitable; however, usability and user workload need improvement. LMP performance exceeded the requirements for system reliability and availability.
- LMP is survivable against an unaided outsider cyber threat having nascent- to limited-level capabilities, but demonstrated it is vulnerable to both nascent- to limited-level insider threats and to an outside threat aided by insiders.
- During the August 1 – 4 , 2016, cybersecurity Verification of Fixes (VoF), LMP demonstrated it had corrected all high- and medium-risk cybersecurity vulnerabilities; however, detect, react, and restore cybersecurity capabilities were not in scope for that event and will be assessed in future cybersecurity testing.
- In support of its 2015 Cyber Economic Vulnerability Assessment (CEVA), the LMP Program Management Office (PMO) chose a commercial vendor that had provided cybersecurity economic subject matter expertise on another Enterprise Resource Planning (ERP) program; however, the vendor's lack of experience regarding LMP and AMC's business processes yielded only high-level findings and recommendations.
- On September 2, 2016, AMC made a full deployment declaration for LMP Increment 2, which will allow the increment to transition to the operation and sustainment phase of the acquisition lifecycle.

System

- LMP is the Army's core logistics Information Technology initiative and is one of the world's largest, fully integrated supply chain, maintenance, repair and overhaul, planning, execution, and financial management systems.
- LMP is an SAP-based commercial off-the-shelf ERP solution that manages and tracks orders and delivery of materiel from the AMC to soldiers where and when they need it.
- LMP transforms Army logistics operations in eight core business areas: acquisition, distribution, finance, product lifecycle management, supply chain planning, depots/arsenals (formerly manufacturing/remanufacturing), maintenance, and warehouse inventory management.
- LMP replaced the two largest national-level logistics systems: the inventory management Commodity Command Standard System, and the depot and arsenal operations Standard Depot System. LMP Increment 2 expands on the already deployed/operational production baseline to specifically address shop floor automation, automatic identification technology, and expanded ammunition requirements. Increment 2 improves outdated or manual processes, updates the other Army ERP systems with relevant information about the Army's military equipment, and provides the tools to support total asset visibility.
- LMP is currently deployed to approximately 30,000 users in more than 50 Army and DOD locations around the world, and interfaces with more than 80 DOD systems.

Mission

The AMC uses LMP to sustain, monitor, measure, and improve the Army's modernized national-level logistics support in order to save Army manpower and money through streamlined activities and greater visibility of logistics operations.

Major Contractors

- CSRA – Fairfax, Virginia
- INSAP Services Inc. – Marlton, New Jersey
- Attain, LLC – McLean, Virginia

Activity

- From September 8 through November 20, 2015, ATEC conducted an adequate IOT&E of the LMP Increment 2 Wave 3 Release 7 at three AMC depots (Corpus Christi Army Depot, Texas; McAlester Army Ammunition Plant, Oklahoma; and Rock Island Arsenal, Illinois). The Army conducted all testing in accordance with a DOT&E-approved test plan.
- Army Research Laboratory's Survivability/Lethality Analysis Directorate conducted a cybersecurity VoF January 19 – 22, 2016, and a follow-up cybersecurity VoF August 1 – 4, 2016.
- On September 2, 2016, the AMC signed a full deployment declaration memorandum for LMP Increment 2, which ends the technical and testing requirements allowing the increment to transition to the operation and sustainment phase of the acquisition lifecycle. DOT&E will continue oversight of LMP's improvements to cybersecurity.
- In FY17, LMP is scheduled to transition its program and data to Defense Information Systems Agency (DISA) Defense Enterprise Computing Centers (DECCs).

Assessment

- LMP is operationally effective.
  - During the IOT&E, users successfully completed 98 percent of the observed Mission Critical Function (MCF)-associated tasks and the Business Operations Test (BOT) confirmed that all but one of the remaining tasks functioned correctly.
  - LMP had no Severity 1 "critical" or Severity 2 "major" problems since the system went live in June 2015. LMP successfully processed more than 99 percent of the more than 1.3 million Intermediate Documents to and from interfacing systems during 2015.
  - Data collectors did not observe some tasks during the IOT&E because the test took place at live, operational locations and users did not perform the tasks over the course of the IOT&E. Data associated with Item Unique Identification (IUID) were not collected because IUID tags have not been placed on all Army logistics items.
  - ATEC assessed LMP Increment 2 as not effective because testers observed only 67 percent of the MCFs during the IOT&E. DOT&E disagrees with the ATEC assessment because testers observed all the missing MCF tasks during the BOT. The BOT involved actual LMP operators using realistic LMP data on a production-representative system.
- LMP is operationally suitable. Users surveyed during the IOT&E rated LMP a mean System Usability Scale score that is representative of "ok" usability and noted their workload remains high because they are using legacy systems concurrently with LMP. This will be the case until LMP completely replaces legacy systems in FY18. LMP demonstrated a Mean Time Between System Failure (MTBSF) of 1,026 hours, which exceeded the requirement of 110 hours MTBSF. LMP had an availability of 96 percent meeting the 95 percent requirement.
- LMP is survivable to an unaided outsider cybersecurity threat having nascent- to limited-level capabilities, but is not survivable to both nascent- to limited-level insider threats and to an outside threat aided by insiders.
- During the August 1 – 4 , 2016, cybersecurity VoF, LMP demonstrated it had corrected all high- and medium-risk cybersecurity vulnerabilities; however, detect, react, and restore cybersecurity capabilities were not in scope for that event and will be assessed in future cybersecurity testing. The remaining low-risk vulnerabilities are either mitigated or will be corrected after LMP migrates to DISA DECCs.
- The 2015 CEVA portion of the LMP cybersecurity testing was inadequate because the LMP PMO chose a commercial vendor that lacked experience with LMP and AMC's business processes and because the vendor failed to conduct a significant portion of the CEVA. Although the vendor had provided cybersecurity economic subject matter expertise on another ERP program, its work during the LMP CEVA yielded only high-level findings and recommendations.
- Although the CEVA was inadequate, the overall test and evaluation of LMP was adequate to support a DOT&E assessment of operational effectiveness, suitability, and survivability.
- During its annual continuity of operations (COOP) test in December 2015, LMP demonstrated the feasibility of, but did not conduct, a transfer of operations to and from the COOP location.
- The 2010 National Defense Authorization Act requires financial audibility by 2017. The Program Office continues to work to achieve certification in accordance with the Federal Financial Management Improvement Act through various audits.

Recommendations

- Status of Previous Recommendations. This is the first annual report for this program.
- FY16 Recommendations. The LMP Program Office should:
  1. Conduct an FOT&E of LMP, focused on IUID and the tasks that were not observed during the IOT&E, when the IUID capability is fully available to LMP users.

2. Continue to survey LMP users to determine if the problem of increased user workload relative to legacy systems is improving.
3. After LMP data and program services transition to DISA DECCs, conduct another cybersecurity test from both the insider and outsider posture to verify the correction of known vulnerabilities and to possibly identify new vulnerabilities.
4. Ensure the cybersecurity economic subject matter experts chosen for the next CEVA understand the operational capabilities and key business processes used within the system to include roles and responsibilities.
5. Use the transition to the DISA DECCs to simulate a full transfer of operations to and from the COOP location.