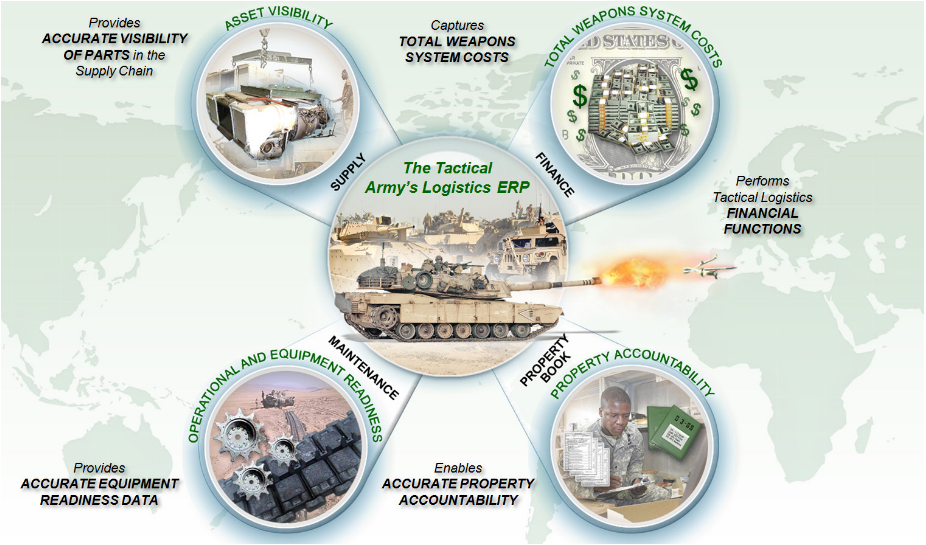
Global Combat Support System – Army (GCSS-Army)


Provides ACCURATE VISIBILITY OF PARTS in the Supply Chain
ASSET VISIBILITY
Captures TOTAL WEAPONS SYSTEM COSTS
TOTAL WEAPONS SYSTEM COSTS
SUPPLY
The Tactical Army's Logistics ERP
FINANCE
Performs Tactical Logistics FINANCIAL FUNCTIONS
MAINTENANCE
PROPERTY BOOK
OPERATIONAL AND EQUIPMENT READINESS
PROPERTY ACCOUNTABILITY
Provides ACCURATE EQUIPMENT READINESS DATA
Enables ACCURATE PROPERTY ACCOUNTABILITY

Executive Summary

- From March 30 to April 10, 2015, DOT&E monitored a Lead Site Verification Test (LSVT) of Wave 2 capability enhancements at two active Army units (2nd Heavy Brigade Combat Team, 1st Armored Division, and 11th Armored Cavalry Regiment); one Army Reserve unit (94th Training Division); and one Army National Guard unit (60th Troop Command).
- From January 2015 through June 2015, DOT&E analyzed system performance data to assess system scalability associated with Material Requirements Planning (MRP) batch jobs as the Army expanded the user base through continued fielding of the Global Combat Support System – Army (GCSS-Army) to additional units.
- GCSS-Army Wave 2 is operationally effective. The system successfully surpassed the 90 percent threshold for all Wave 2 critical mission functions attempted by users. Reports generated at all levels provided leaders with essential decision-making information to support force maintenance and sustainment.
- GCSS-Army is operationally suitable, with usability and resolution of help desk tickets needing some improvement. GCSS-Army exceeded the requirements for system reliability and availability.
- The system is survivable against an intermediate-level outsider threat, but is vulnerable to an intermediate-level insider cyber threat. Survivability against an advanced persistent outsider cyber threat was not tested.
- The GCSS-Army program continues to make progress in support of the legislative mandate to be financially auditable by 2017.

System

- GCSS-Army is an information technology system based on commercial off-the-shelf and government off-the-shelf software and hardware.
- GCSS-Army uses an adaptation of a commercially-available Enterprise Resource Planning system to integrate internal and external management information across an organization, including finance/accounting, manufacturing, sales and service, and customer relationship management. GCSS-Army centralizes and standardizes these activities and provides automation to assist users with common tasks, such as reporting.
- The hardware component of GCSS-Army is located on production servers in Redstone, Alabama, and Continuity of Operations servers in Radford, Virginia.
- The GCSS-Army program includes the Army Enterprise Systems Integration Program that provides the enterprise hub services, centralized master data management, and cross-functional business intelligence and analytics for Army Enterprise Resource Planning solutions, including the General Fund Enterprise Business System and Logistics Modernization Program.
- The Army is fielding GCSS-Army in two waves:
    - Wave 1 contains the retail supply and associated financial functions and will be completed in 2QFY16.
    - Wave 2 contains the remaining functions and will be fielded in FY16-17.
- GCSS-Army executes financial actions and is therefore subject to the 2010 National Defense Authorization Act requirement to be auditable by 2017.

Mission

Army logisticians use GCSS-Army to view, access, and exchange consolidated operational logistics data to conduct maintenance, material management, property accountability, financial management, and logistics planning.

Major Contractors

- Northrop Grumman Space and Mission Systems Division – Bon Air, Virginia
- LMI Consulting – McLean, Virginia
- InSAP Services, Inc. – Marlton, New Jersey

Activity

- The Army Research Laboratory Survivability/Lethality Analysis Directorate conducted cybersecurity vulnerability and penetration assessment testing of GCSS-Army in January 2015 in accordance with a DOT&E-approved test plan. The purpose of this testing was to identify vulnerabilities and allow time to fix them prior to a full-scope Adversarial Assessment and Cyber Economic Vulnerability Assessment.
- From January 2015 through June 2015, DOT&E analyzed system performance data to assess system scalability associated with MRP batch jobs as the Army expanded the user base through continued fielding of GCSS-Army to additional units.
- A Red Team from the Army's Threat Systems Management Office (TSMO) conducted a full-scope cybersecurity Adversarial Assessment and cyber economic vulnerability testing of GCSS-Army in February 2015. TSMO received support from a commercial financial auditing team for the cyber economic vulnerability testing.
- From February 23 through March 13, 2015, DOT&E observed independent government testing of deployment/redeployment functionality to and from both mature and immature theaters of operation. This was an integrated developmental test/operational test conducted at Fort Lee, Virginia, with Active Duty and Army National Guard Soldiers using the Program Office's developmental test client.
- From March 23 through April 10, 2015, DOT&E monitored an LSVT of Wave 2 capability enhancements at two active Army units (2nd Heavy Brigade Combat Team, 1st Armored Division at Fort Bliss, Texas, and 11th Armored Cavalry Regiment at Fort Irwin, California); one Army Reserve unit (94th Training Division at Fort Bragg, North Carolina); and one Army National Guard unit (60th Troop Command, Raleigh, North Carolina). This was an independent operational test involving typical users in an operationally realistic environment to assess specific risk factors for operational effectiveness, operational suitability, and survivability.
- From May 26 through June 9, 2015, the Army Test and Evaluation Command (ATEC) witnessed independent government testing of disconnected automated identification technology capabilities at the Program Management Office's facility in Petersburg, Virginia. This technology allows GCSS-Army users to conduct limited supply operations without an active communications network.
- From August 17 through September 3, 2015, ATEC reviewed the end-to-end deployment/redeployment standard operating procedure documentation at the Program Office's facility in Petersburg, Virginia. This documentation will be used by Army commanders to orchestrate deployment processes using GCSS-Army. Additionally, ATEC observed follow-on independent government testing of disconnected automated identification technology capabilities.
- A full transfer of operations to and from the continuity of operations location was not tested.
- DOT&E submitted an FOT&E report in November 2015 on the LSVT.

Assessment

- GCSS-Army Wave 2 is operationally effective.
  - The system successfully surpassed the 90 percent threshold for all Wave 2 critical mission functions attempted by users.
  - Reports generated at all levels provided leaders with essential decision-making information to support force maintenance and sustainment. However, users noted that some maintenance, finance, and logistics management reports took longer than expected to run or they timed out before completion, causing users to spend more time with multiple transaction attempts.
  - Server capacity can support continued Wave 1 fielding and the continuation of upgrades from Wave 1 to Wave 2.
  - During the LSVT, the new interface between GCSS-Army and the legacy Standard Army Management Information System systems for property book, maintenance, and unit supply worked properly.
- GCSS-Army is operationally suitable, with usability and resolution of help desk tickets needing some improvement. GCSS-Army exceeded the requirements for system reliability and availability.
- GCSS-Army was shown to be survivable against an intermediate-level outsider cyber threat, but was vulnerable to an intermediate-level insider cyber threat. Survivability against an advanced persistent outsider cyber threat using specialized tools or exploits was not tested. GCSS-Army has improved its cybersecurity capabilities since earlier testing.
- GCSS-Army demonstrated the ability to detect and react to cyber threats in support of the operational mission, data, and users. A Cyber Economic Vulnerability Assessment, performed as a table-top assessment based on vulnerabilities discovered and exploited during the Adversarial Assessment, did not reveal any additional significant risks. While analysis shows that the MRP reports are running slightly longer, it is not indicative of a capacity shortfall.
- During the migration to GCSS-Army Wave 2, the number of units running reports and the number of reports they are running was expected to increase. The weekly MRP report data provides the Program Office the ability to predict any future need to upgrade its servers to handle the increasing report processing workload.
- The 2010 National Defense Authorization Act requires financial audibility by 2017. GCSS-Army continues to work to achieve certification in accordance with the Federal Financial Management Improvement Act through various audits.

Recommendations

- Status of Previous Recommendations. The GCSS-Army program manager has addressed all previous recommendations and continues to make progress in support of meeting the legislative mandate to be financially auditable by 2017.
- FY15 Recommendation.
  1. The GCSS-Army Program Office should conduct a full transfer of operations to and from the continuity of operations location.