Global Combat Support System – Joint (GCSS-J)

Executive Summary

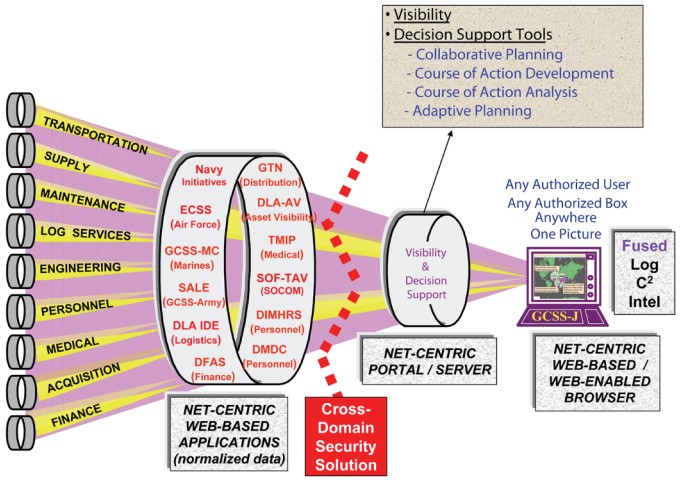
- The Joint Interoperability Test Command (JITC) conducted a risk assessment for each version of the software and recommended a level of test for DOT&E approval. DOT&E approved the plan for a full operational test for Global Combat Support System – Joint (GCSS-J) version 7.1.0. Because of lower risks for versions 7.1.1 and 7.1.2, DOT&E approved the plan for operational assessments based on JITC's observation of the developmental tests conducted by the program manager.
- The latest version, 7.1.2, is operationally effective and operationally suitable. The application is survivable against cyber attacks. The primary host server site, however, did not meet the required level of cyber attack detection measures.

System

- The GCSS-J is a web portal that enables users at combatant commands and joint task forces to access joint logistics applications.
- The system supports planning, execution, and control for engineering, health services, logistics services, supply, distribution, and maintenance operations. It is comprised of strategic servers (located in Montgomery, Alabama, and Pearl Harbor, Hawaii), a commercial off-the-shelf-based infrastructure, and Public Key Infrastructure.
- GCSS-J supports the situational awareness of the military operators by providing applications for the following: search, query, and reports capability; Watchboard (allowing rapid comparison of planned actions with actual events); electronic battlebook (organizing files and web pages into categories); knowledge management; business intelligence; mapping capability; joint engineer planning; and execution capability.
- GCSS-J Increment 7 follows an agile acquisition strategy that supports multiple releases of the updated software in coordination with the user, program manager, and testers. In 2010, the Defense Information Systems Agency (DISA) released three versions of GCSS-J: 7.1.0, 7.1.1, and 7.1.2.

Mission

- Joint commanders use GCSS-J to move and sustain joint forces throughout the entire spectrum of military operations.



C² - Command and Control
DFAS - Defense Finance and Accounting Service
DIMHRS - Defense Integrated Military Human Resources System
DLA-AV - Defense Logistics Agency - Asset Visibility
DLA-IDE - Defense Logistics Agency - Integrated Data Environment
DMDC - Defense Manpower Data Center
ECSS - Expeditionary Combat Support System
GCSS-Army - Global Combat Support System-Army
GCSS-MC - Global Combat Support System-Marine Corps
GCSS-Navy - Global Combat Support System-Navy
GTN - Global Transportation Network
IDE-AV - Integrated Data Environment - Asset Visibility
SALE - Single Army Logistics Enterprise
SIPRNET - Secret Internet Protocol Routed Network
SOCOM - Special Operations Command
SOF-TAV - Special Operations Forces - Total Asset Visibility
TMIP - Theater Medical Information Program

- Combatant Command and Joint Task Force commanders and logistics staffs use the GCSS-J to gain end-to-end visibility of combat support capability up through the strategic level, facilitating information flow across and between combat support and command and control functions.

Major Contractor

Northrop Grumman Mission Systems – Herndon, Virginia

Activity

- JITC conducted a risk assessment for each version of the software and recommended a level of test for DOT&E approval. DOT&E approved the plan for a full operational test for version 7.1.0. Because of lower risks for versions 7.1.1 and 7.1.2, DOT&E approved the plan for operational assessments based on JITC's observation of the developmental tests conducted by the program manager.
- JITC conducted an operational test of GCSS-J version 7.1.0 from October 20 through November 3, 2009, in accordance with the DOT&E-approved test plan.

- JITC assessed GCSS-J version 7.1.1 Secret Internet Protocol Router Network (SIPRNet) based on participation in the developmental test conducted from February 22 to April 22, 2010. JITC conducted a separate operational test at the primary hosting site in Montgomery, Alabama, March 8 - 19, 2010, to assess operational survivability against cyber attacks.
- JITC assessed GCSS-J version 7.1.2 using the results from the developmental tests conducted by the program manager in accordance with the risk assessment recommendations. The SIPRNet GCSS-J version 7.1.2 developmental test was from July 26 through August 3, 2010, and Unclassified but Sensitive Internet protocol Router Network (NIPRNet) version 7.1.2 developmental test was September 3 - 7, 2010.

Assessment

- GCSS-J version 7.1.0 was operationally effective. It incorporates an improved Query Tool. The Joint Logistics Management functional areas incorporated tools providing improved user visibility into the status of ammunition inventories and allowed easier interface with query tools and the Watchboard. Maintenance, Supply and Services, Movement, Personnel Management, and Health Services functional areas were operationally effective. However, the Joint Engineering Planning and Execution System had critical problems, making that function not operationally effective.
- GCSS-J version 7.1.0 was operationally suitable, with good training and good system reliability and availability. The performance of the help desk showed improvement. Evaluation of IA was limited. IA controls associated with protect, detect, react, and restore at the application level were satisfactory, but IA controls at the server level could not be assessed. DOT&E agreed to defer a vulnerability assessment of the DISA host server suite to the 7.1.1 operational test.
- GCSS-J version 7.1.1 corrected errors discovered in operational testing of GCSS-J version 7.1.0, and the system was assessed to be operationally effective and suitable. A separate vulnerability assessment of the DISA host server suite revealed that GCSS-J version 7.1.1 did not add significant vulnerability against cyber attacks, but that the primary host site in Montgomery, Alabama, could not detect the cyber attacks to the required level.
- Both the SIPRNet and NIPRNet version 7.1.2 are operationally effective and operationally suitable. Like version 7.1.1, version 7.1.2 does not cause an unacceptable increase in vulnerability of the DISA network. However, the primary host site must make additional improvements toward meeting the required level of cyber attack detection measures.

Recommendations

- Status of Previous Recommendations. DISA has taken appropriate action on the previous recommendations.
- FY10 Recommendation.
  1. DISA should improve the security posture of the server hosting sites and perform penetration tests on an annual basis.