DOD PROGRAMS

Global Combat Support System Combatant Commanders / Joint Task Force (GCSS CC/JTF)

Executive Summary

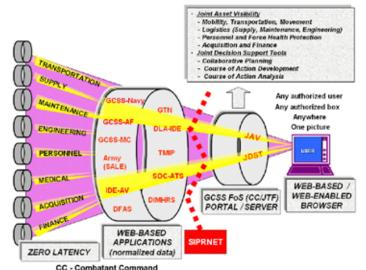
- The Joint Interoperability Test Command (JITC) conducted an IOT&E for Global Combat Support System Combatant Commanders / Joint Task Force (GCSS CC/JTF) version 6.0 in November 2006 and identified several deficiencies with suitability and survivability. All deficiencies were satisfactorily resolved and version 6.0 received a favorable fielding decision in January 2007.
- Version 6.1 adds new capabilities such as the ability to use Non-secure Internet Protocol Router Network (NIPRNET) as well as improving the user interfaces through incorporation of commercial off-the-shelf (COTS) products.
- JITC will operationally test GCSS CC/JTF version 6.1 in FY08.

System

- GCSS CC/JTF is a web portal that enables users at combatant command and joint task force to access joint logistics applications.
- The system is comprised of strategic servers located in Montgomery, Alabama, and Pearl Harbor, Hawaii, a COTS-based infrastructure, and Public Key Infrastructure (PKI) enabled capabilities that support planning, execution, and control for engineering, health services, logistics services, supply, and distribution.
- GCSS CC/JTF provides the following applications: reports capability; watchboard (allowing rapid comparison of planned actions with actual event); electronic battlebook (organizing files and web pages into categories), knowledge management; business intelligence; mapping capability; joint engineer planning; and execution capability.

Mission

 Joint commanders use GCSS CC/JTF to move and sustain joint forces throughout the entire spectrum of military operations.



DFAS - Defense Finance and Accounting Service
DIMHRS - Defense Integrated Military Human Resources Syste,
DLA-IDE - Defense Logistics Agency - Integrated Data Environment
FoS - Family of Systems
GCSS-AF - Global Combat Support System-Air Force
GCSS-Macy - Global Combat Support System-Marine Corps
GCSS-Navy - Global Combat Support System-Navy
GTN - Global Transportation Network
IDE-AV - Integrated Data Environment - Asset Visibility
JAV - Joint Asset Visibility
JDST - Joint Decision Support Tool
JTF - Joint Decision Support Tool
JTF - Joint Task Force
SALE - Single Army Logistics Enterprise
SIPRNET - Secret Internet Protocol Routed Network
SOC-ATS - Special Operationis Command - Asset Tracking System
TMIP - Theater Medical Information Program

 Combatant Command and Joint Task Force commanders and logistics staffs use the GSS CC/JTF to gain end-to-end visibility of Combat Support (CS) capability up through strategic level, facilitating information flow across and between CS and command and control functions.

Activity

JITC completed operational testing of GCSS CC/JTF version 6.0 on November 17, 2006. Testing occurred at two Defense Enterprise Computing Center operational server sites (Montgomery, Alabama, and Pearl Harbor, Hawaii) with users located at U.S. Central Command (CENTCOM), U.S. Southern Command (SOUTHCOM), and the Defense Information Systems Agency (DISA) Eagle building. Participants included CENTCOM, U.S.

European Command (EUCOM), U.S. Joint Forces Command (JFCOM), U.S. Northern Command (NORTHCOM), U.S. Pacific Command (PACOM), SOUTHCOM, U.S. Strategic Command (STRATCOM), U.S. Transportation Command (TRANSCOM), the Joint Staff (J4), and the 416th Engineering Command representatives. JITC conducted a limited test to assess the alternate server's ability to take control from the primary server on November 22, 2006.

DOD PROGRAMS

- JITC and the Defense Intelligence Agency concluded security testing of GCSS CC/JTF v6.0 on October 13, 2006, with a follow-on Security Test and Evaluation completed on December 15, 2006.
- Operational testing of GCSS CC/JTF version 6.1 was deferred from September 2007 until FY08.

Assessment

- Operational testing of GCSS CC/JTF 6.0 was adequate.
- Primary and Back-up version 6.0 suites were fully functional with access to authoritative data sources. Enterprise Systems Management support provided centralized processes/tools for systems administration and visibility on the health and status of the system.
- Testers were successful in demonstrating mission accomplishment using the new capabilities. All critical interfaces performed satisfactorily.
- JITC evaluated GCSS CC/JTF version 6.0 to be operationally effective and suitable, but not survivable due to critical information assurance deficiencies. After successful mitigation of the critical Information Assurance deficiencies

- and downgrading of the system to Mission Assurance Category (MAC) II, the Designated Approving Authority granted an Authority to Operate, and the Milestone Decision Authority approved fielding of version 6.0.
- The automated failover process for switching users from the primary server in Montgomery, Alabama, to the secondary server located in Pearl Harbor, Hawaii, was not implemented. This shortfall requires users to switch over manually; however, the manual switch over can be completed within the required time for a MAC II system.

Recommendations

- Status of Previous Recommendations. There are no previous recommendations.
- FY07 Recommendations. The GCSS CC/JTF program manager should:
 - 1. Implement automated failover processes for full compliance as a MAC II system.
 - 2. Continue to develop and field corrections for remaining Information Assurance findings.