

GLOBAL COMBAT AND SUPPORT SYSTEM (GCSS)



DISA ACAT IAM Program

Total Number of Systems:	50 sites
Total Program Cost (TY\$):	\$310M
Life-Cycle Cost (TY\$):	\$57M
Full-rate production:	1QFY01

Prime Contractor

DISA Defense Enterprise Integration Services

SYSTEM DESCRIPTION & CONTRIBUTION TO JOINT VISION 2020

The Global Combat Support System (GCSS) contributes to *decision superiority* and *focused logistics* in *Joint Vision 2020* by providing top-level commanders and planners current integrated logistics and combat support information from either their workstation web browser (GCSS-Portal) or via a drill-down tool within the Common Operating Picture, Combat Support Enhanced (COP-CSE) display. It supports *interoperability* by accessing key data bases: Joint Total Asset Visibility (JTAV), Global Transportation Network (GTN), Global Status of Resources and Training System (GSORTS), Joint Operational Planning and Execution System (JOPES), and Units, Sites, Tracks Data Store (USTDS) extract from the National Imagery and Mapping Agency (NIMA). GCSS servers employ coded queries to retrieve data as needed from the source data bases, but they neither store nor alter the source data. GCSS taps commercial *innovation* by employing commercial standards and software, and by riding on the Common Operating Environment, which has become the server level of the Defense Information Infrastructure (DII). The DII itself employs Internet technology communications of the Secret Internet Protocol Router Network (SIPRNET).

BACKGROUND INFORMATION

For over a year, several components at Pacific Command (PACOM) have been using a demonstration suite of GCSS. Although the prototype system has not yet been fielded as an integrated element of the Global Command and Control System (GCCS), it has been able to access the true source data bases directly over the SIPRNET to support tests and exercises. This year's OT&E of GCSS v2.0 was to assist the Joint Staff, J-4, in deciding how and whether to field GCSS. The fielding would place GCSS servers under Defense Information Systems Agency (DISA) management at four CINCs, while users would access GCSS information via COP-CSE and GCSS-Portal installed on their workstations within the GCCS environment.

Future versions of GCSS will have terminals outside GCCS and employ some Sensitive But Unclassified information exchanges over the Not Classified Internet Protocol Network (NIPRNET). Since initial user access to GCSS was to be entirely within the GCCS suite at each CINC, the GCSS TEMP for GCSS v2.0 was developed and approved as an Annex to the Capstone GCCS TEMP. Next year, a standalone GCSS Capstone TEMP will be written for the more independent future versions.

TEST & EVALUATION ACTIVITY

The first phase of OT&E was conducted at four PACOM locations: US Pacific Fleet, U.S. Marine Forces Pacific, U.S. Air Force Pacific, and U.S. Army Pacific Headquarters. Although OT&E was conducted on prototype GCSS systems on a shadow GCCS network, the test team observed GCSS being reinstalled as if for the first time and also observed the training of the ten users, most of whom were new to GCSS. A second phase of OT&E will be conducted at the next CONUS CINC to install GCSS. This phase will be conducted on a fully operational network with GCSS loaded as a mission application on operational GCCS systems. When complete, OT&E will evaluate operational effectiveness and suitability based on mission performance, interoperability, security, and mission support and supportability, which include usability and sustainment.

The Joint Interoperability Test Command first observed and verified installation and then conducted the functional portion of the OT&E of GCSS from September 27-October 5, 2000. Following the functional testing, the Joint Staff, J6K, and National Security Agency conducted the Security Test and Evaluation (ST&E) part of OT&E from October 4-18. For the functional testing, users employed GCCS to display facilities and deployments and to answer logistics questions with GCSS queries. In order to verify that the information presented to its users by GCSS agreed with that in the authoritative source data bases, Subject Matter Experts (SMEs) retrieved the comparable information directly from those data bases. Tests for continuity of operations consisted of disabling the connection to the GTN data base and shutting down the GCSS server. Numerous test deviations occurred. The most significant deviation was the last minute inclusion of more representative, less capable workstations, some of which were located in the GCCS environment to validate the ST&E test configuration.

TEST & EVALUATION ASSESSMENT

This first phase of OT&E proved insufficient to evaluate operational effectiveness or suitability. The security testing revealed discrepancies in the installed GCSS configuration and significant security vulnerabilities for GCSS and its source data bases. Before the test, the test team was concerned that the beta site users would be overly experienced, but the opposite occurred. According to survey comments and observed difficulties in querying GCSS, the limited four-hour training sessions were inadequate for most GCSS users. During the test, users had high confidence on less than 75 percent for GCSS-Portal trials and only 65 percent of the COP-CSE trials. In most of the low confidence trials, users got no information back from GCSS. Even the most experienced users had little confidence in 20 percent of their results. Less than half of the users preferred GCSS to their current methods, found it useful, or would use it on a daily basis if available. Because of the complexity of the conditions placed on queries, such as time ranges, the SMEs retrieved usable comparison information for less than one-quarter of the queries coded into GCSS. This small sample could not assure that 95 percent of the queries were error free with 80 percent confidence. Moreover, one of the two significant Test Incident Reports revealed a programming error in a coded query. While users could report problems to the help desk and GCSS recovered within two hours, which is satisfactory for GCSS, help procedures should be streamlined and rely more on local GCSS system administrators.

CONCLUSIONS, RECOMMENDATIONS AND LESSONS LEARNED

Although the first phase of OT&E was inconclusive, it did not reveal any technical reason that GCSS 2.0 should not be installed at another test site for the second phase of OT&E. Security protections, configuration control, and installation procedures must be improved before re-testing security or performing the second phase of OT&E. To evaluate GCSS performance, testers must know how sites expect GCSS to conduct their missions. For example, testers must know whether only specialists and experts are to use GCSS and, since the data bases themselves are known to be imperfect, whether GCSS is only intended to give preliminary results that will be verified by other means. Once the intended users are identified and their missions are understood, training for the second phase must be specific to the user tasks and in sufficient depth to determine whether typical users can select the proper queries and properly execute them for their intended tasks. The user procedures and coded queries should also be reviewed for clarity and accuracy, and any problems should be assessed for their operational impact.

