

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.