Global Command & Control System – Joint (GCCS-J)

GLOBAL COMMAND & CONTROL SYSTEM - JOINT (GCCS-J)
DEFENSE INFORMATION SYSTEMS AGENCY

The Global Command & Control System – Joint (GCCS-J) family of systems has been broken into two separate acquisition programs: GCCS-J and Joint Planning and Execution System, which is being reported on in a separate article. In FY23, GCCS-J fielded v6.1.0.0, providing a significant upgrade to the GCCS-J program. DOT&E is analyzing data collected during operational testing in FY23, plans to observe further testing in FY24, and will report on operational effectiveness, suitability, and cyber survivability in 3QFY24.

SYSTEM DESCRIPTION

GCCS-J is a software-based system with commercial off-the-shelf and government off-the-shelf software and is highly modular, allowing the deployed configuration to be customized to fit each deployed sites' requirements. The GCCS-J system uses procedures, standards, and interfaces that provide an integrated, near real-time picture of the battlespace that is necessary to conduct joint and multi-national operations.

MISSION

GCCS-J enables joint commanders to accomplish command and control by:

- Displaying geographic track information integrated with available intelligence and environmental information to provide the user a fused battlespace picture;
- Providing integrated imagery and intelligence capabilities (e.g., battlespace- views and other relevant intelligence) into the common operational picture (COP); and
- Providing a missile warning and tracking capability.

PROGRAM

The GCCS-J Program Management Office (PMO) fielded version v6.1.0.0 as a significant upgrade to the existing fielded version of v6.0.1.x. During FY23 operational testing, users identified impactful upgrades that have been added for future development. As the PMO continues development of the v6.1.x baseline, GCCS-J will field user-identified capabilities through the Development, Security, and Operations (DevSecOps) process as part of their Agile software development framework.

» MAJOR CONTRACTORS

- Northrop Grumman Systems Corporation – San Diego, California
- NextGen Federal Systems – Annapolis Junction, Maryland

TEST ADEQUACY

In FY23, the Joint Interoperability Test Command (JITC) conducted one operational test which was observed by DOT&E, for GCCS-J v6.1.0.x. The GCCS-J v6.1.0.0 Operational Test included representative hardware, software, real-world data, and operational end users that exercised system administration, COP, and intelligence user mission tasks. Testing focused on the capabilities and interfaces available at U.S Central Command (USCENTCOM) and U.S. Southern Command (USSOUTHCOM). Test cases were developed with direct input from users at both combatant commands. Additional combatant and lower echelon commands with site specific test cases will be tested as these commands migrate to v6.1.0.x.

The GCCS-J integrated test environment does not currently capture the mission configurations associated with each Combatant Command and other critical sites. As reported in the FY22 Annual Report, GCCS-J test strategies need to be developed to encompass the agile nature of the product and varying operational site configurations to inform the update to the Test and Evaluation Master Plan (TEMP) and the Agile Operational Master Test Plan (AOMTP). Additionally, the TEMP update for the GCCS-J program should detail operational cyber survivability tests that include cooperative vulnerability and penetration assessments (CVPAs) followed by adversarial assessments (AAs).

PERFORMANCE

» EFFECTIVENESS AND SUITABILITY

DOT&E is assessing the data from the GCCS-J operational testing in FY23 and will report on operational effectiveness, suitability, and cyber survivability in FY24 following completion of additional operational testing.

» SURVIVABILITY

DISA has not conducted operational cyber survivability testing of v6.1.x and should conduct a CVPA and an AA to complete the testing necessary to support an evaluation of cyber survivability.

RECOMMENDATIONS

DISA should:

1. Develop test strategies to encompass the agile nature and varying operational site configurations to inform the update to the TEMP and the AOMTP, as discussed in the FY22 Annual Report.
2. Conduct a CVPA and an AA to complete testing necessary to support an evaluation of cyber survivability.