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

In FY23, the Global Command & Control System – Joint (GCCS-J) Program Management Office (PMO) fielded GCCS-J version v6.1.0.0, delivering a significant infrastructure upgrade to the GCCS-J program. However, v6.1.0.0 did not have all of the capabilities of the fielded version, v6.0.1.30. GCCS-J v6.1.0.4, which has all of the capabilities of v6.0.1.30, was not ready for operational test in FY24. Therefore, the FOT&E of v6.1.0.4 will be reported in 3QFY25 – a one-year slip from what DOT&E reported in the FY23 Annual Report.

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 customization of the deployed configuration 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

Joint commanders use GCCS-J 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

In FY23, the GCCS-J PMO fielded version v6.1.0.0 as a significant upgrade to the existing fielded version of v6.0.1.30. However, v6.1.0.0 did not capture all of the capabilities of the v6.0.1.30, and due to delays in command transitions to v6.1.0.4, FOT&E is planned to be completed in 1QFY25. DOT&E will publish an FOT&E report in 3QFY25. User sites choose when to upgrade GCCS-J for use in military operations. During operational testing, users identified impactful improvements that will be added into future GCCS-J development requirements. As the PMO continues software development, GCCS-J will field user-identified capabilities through the Development Security Operations (DevSecOps) process as part of their Agile software development framework.

» MAJOR CONTRACTORS

- Northrop Grumman Systems Corporation – Newport News, Virginia
- NextGen Federal Systems – Annapolis Junction, Maryland

TEST ADEQUACY

In FY23, the Joint Interoperability Test Command (JITC) conducted one operational test of GCCS-J v6.1.0.0. The test was conducted in accordance with DOT&E guidance and observed by DOT&E and 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. In 1QFY25, FOT&E is planned to be conducted with commands at U.S. Army Pacific and U.S. Marine Corps Forces, Pacific, with site-specific test cases as these commands migrate to v6.1.0.4.

The GCCS-J integrated test environment does not currently capture the mission configurations associated with each combatant command and other critical sites. GCCS-J test strategies need to be developed to encompass the agile nature of the product and varying operational site configurations, to inform updates to the TEMP and Agile Operational Test Plan (AOTP). Moreover, the TEMP update 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 will continue to assess data from the GCCS-J FOT&E of v6.1.0.4, which is scheduled to complete in FY25. DOT&E will report on operational effectiveness and suitability upon completion of FOT&E.

» SURVIVABILITY

JITC has not conducted operational cyber survivability

testing of v6.1.0.4 and should conduct a CVPA and an AA to complete the testing necessary to support an evaluation of cyber survivability. DOT&E will report on cyber survivability upon completion of FOT&E.

RECOMMENDATIONS

Defense Information Systems Agency (DISA) should:

1. Develop test strategies to encompass the agile nature and varying operational site configurations to inform the updates to the TEMP and AOTP, which must be submitted to DOT&E for approval, as discussed in the FY22 and FY23 Annual Reports.
2. Conduct a CVPA and an AA to complete testing necessary to support an evaluation of cyber survivability, as discussed in the FY23 Annual Report.