

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

Executive Summary

- In FY19, the Global Command and Control System – Joint (GCCS-J) Program Manager focused on the sustainment of the existing fielded GCCS-J v4.3.x baseline and the development of GCCS-J v6.x and a new modernized GCCS-J. The Joint Planning and Execution Services (JPES) Program Manager focused on sustaining the existing fielded Joint Operation Planning and Execution System (JOPES) v4.3 baseline and development of JPES.

GCCS-J Operations (formerly named GCCS-J Global)

- The GCCS-J v6.0.1.0 OT&E, in September 2018, showed that the system was not operationally effective and not operationally suitable.
- Following the OT&E, the Command and Control (C2) Executive Steering Council (ESC) directed DISA to field the updated GCCS-J v6.0.1.2, with defect fixes, to three Joint Staff J3-identified Combatant Commands and the Joint Staff Support Center (JSSC) in order to conduct additional testing to validate OT&E fixes and to determine system stability in the operational environment.
- The GCCS-J v6.0.1.2 Operational Assessment (OA) in March 2019 showed that the system is not operationally effective or operationally suitable, nor was the system stable in the operational environment.
- Following the GCCS-J v6.0.1.2 OA, DISA fielded an Emergency Release to resolve 6 of the 10 Priority 2 defects discovered during the OA. The Program Office plans to field a number of Maintenance Releases (MRs) prior to September 2020 to address the remaining system defects.
- Despite poor test results, the C2 ESC declared GCCS-J v6.0.1.x operationally viable and ready for operational use beginning September 1, 2019. Users can choose not to use the new version of GCCS-J because the old version is still fielded. However, the C2 ESC ready for operational use determination started the 1-year sunset clock for the currently fielded GCCS-J v4.3.

GCCS-J Modernization (formerly named GCCS-J Joint Enterprise)

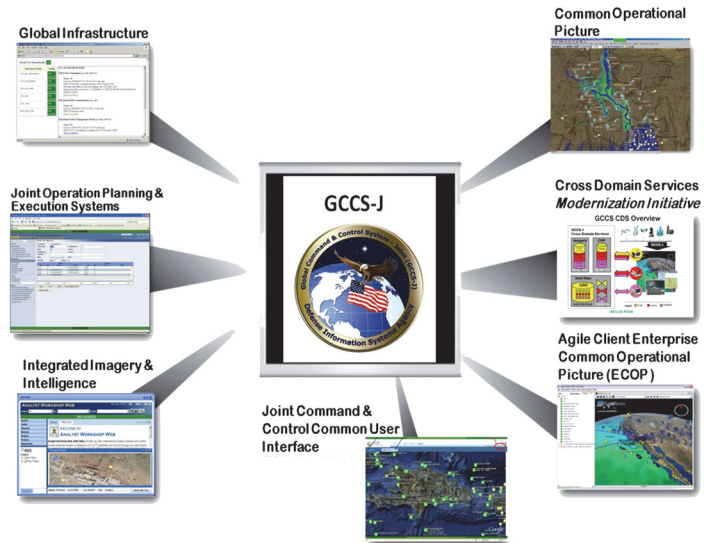
- The Program Office released three Program Increments (PI) in FY19, using “agile” development processes. User feedback from limited user assessments of each PI was mostly positive; however, users observed that many capabilities required additional development.

JPES

- DISA is rebaselining the JPES program and plans to extend legacy JOPES sustainment through 2022.

System

GCCS-J consists of hardware, software (both commercial off-the-shelf and government off-the-shelf), 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. Its client/server architecture uses open systems standards and government-developed military planning software. GCCS-J Operations, GCCS-J Modernization, and JPES are the three systems that comprise GCCS-J.

GCCS-J Operations

- GCCS-J v6.0.1.2 is intended to provide back-end services, databases, and system administration functions. Agile Client v5.2.0.2 is intended to provide visualization and presentation of GCCS-J mission applications and functionality to the user. The Program Office is using agile development to evolve Global v6.0.1.2, using incremental MRs to expand capabilities available to the warfighter.

GCCS-J Modernization

- GCCS-J Modernization is intended to be a state-of-the-art information technology solution that replaces the currently operating GCCS-J systems with one enterprise, cloud instance on a global scale. It will provide the warfighter C2 situational awareness via a common operational picture and intelligence products. The Program Office is using “agile” software processes to develop GCCS-J Modernization, releasing PIs to expand capabilities available to the warfighter. GCCS-J Modernization is intended to replace GCCS-J v6.x and Agile Client v5.2.0.2.

JPES

- DISA is developing JPES to replace the legacy JOPES v4.3 baseline. JPES provides all of the functionality of the current JOPES in a modernized architecture.
- DISA is implementing a JPES Framework to support dual operations, as users transition from JOPES to JPES. The JPES Framework is a suite of infrastructure services that enable information exchanges between the JOPES and two

non-critical Global Force Management applications: the Joint Capabilities Requirements Manager (JCRM) and Preferred Force Generator (PFG).

Mission

Joint Commanders utilize the GCCS-J to accomplish C2.

GCCS-J Operations and Modernization

- Commanders use GCCS-J to:
 - Link the National Command Authority to the Joint Task Force, Component Commanders, and Service-unique systems at lower levels of command
 - Process, correlate, and display geographic track information integrated with available intelligence and environmental information to provide the user a fused battlespace picture
 - Provide integrated imagery and intelligence capabilities (e.g., battlespace views and other relevant intelligence) into the common operational picture and allow commanders to manage and produce target data using the joint tactical terminal
 - Provide a missile warning and tracking capability
- Air Operations Centers use GCCS-J to:

- Build the air picture portion of the common operational picture
- Correlate or merge raw track data from multiple sources
- Associate raw electronics intelligence data with track data
- Perform targeting operations

JPES

- Commanders use JPES to:
 - Translate policy decisions into operations plans that meet U.S. requirements to employ military forces
 - Support force deployment
 - Conduct contingency and crisis action planning

Major Contractors

- Government Integrator: DISA – Fort Meade, Maryland
- Software Developers:
 - Northrop Grumman – Arlington, Virginia
 - Leidos – Arlington, Virginia
 - InterImage – Arlington, Virginia
 - CSRA – Falls Church, Virginia

Activity

GCCS-J Operations

- The Program Office approved the following releases in FY19:
 - v6.0.1.1 MR in December 2018
 - v6.0.1.2 MR in February 2019
 - v6.0.1.2 MR in April 2019
 - v6.0.1.3 MR in June 2019
- The Joint Interoperability Test Command (JITC) conducted the GCCS-J v6.0.1.0 level II operational test at U.S. Central Command (USCENTCOM) and U.S. Indo-Pacific Command (USINDOPACOM) September 17 – 28, 2018, in accordance with a DOT&E-approved test plan.
- The C2 ESC determined that GCCS-J v6.0.1.0 was not ready for operational use on December 18, 2018.
- JITC conducted the GCCS-J v6.0.1.2 OA at USCENTCOM Headquarters, MacDill AFB, Florida; USINDOPACOM Headquarters, Camp H. M. Smith, Hawaii; U.S. Strategic Command (USSTRATCOM) Headquarters, Offutt AFB, Nebraska; and the JSSC, Defense Pentagon, Washington, D.C., from March through May 2019, in accordance with a DOT&E-approved test plan.
- Following the GCCS-J v6.0.1.2 OA, DISA fielded an Emergency Release to resolve 6 of the 10 Priority 2 defects discovered during the OA. The GCCS-J Program Office plans to field a number of MRs prior to September 2020 to address the remaining system defects. JITC plans to assess Program Office defect fixes in future MRs.
- Despite poor reliability, the C2 ESC declared GCCS-J v6.0.1.x operationally viable and ready for operational use beginning September 1, 2019. The C2 ESC ready for

operational use determination started the one-year sunset clock for the currently fielded GCCS-J v4.3.

- DOT&E released the report on the GCCS-J OA in November 2019.
- JITC is planning to conduct GCCS-J v6.0.1.2 cybersecurity testing in the first half of 2020.

GCCS-J Modernization

- The Program Office approved the following releases in FY19:
 - Modernization PI-1 in March 2019
 - Modernization PI-2 in June 2019
 - Modernization PI-3 in August 2019
- The Program Office conducted a system demonstration for each of the GCCS-J Modernization PIs prior to Government acceptance in March, June, and August 2019.
- JITC conducted a limited user assessment at the end of each GCCS-J Modernization PI to verify user-facing capabilities and collect user feedback in March, June, and August 2019.

JPES

- DISA is rebaselining the JPES program and plans to extend legacy JOPES sustainment through 2022.
- The Program Office and JITC conducted a JPES Framework Risk Reduction Event (RRE) at the Joint Staff J35, Norfolk, Virginia, and JSSC, Pentagon, Washington D.C., August 19 – 23, 2019. The purpose of the RRE was to evaluate JPES framework suitability in the operational environment and to reduce program risk prior to the JPES IOT&E.

Assessment

GCCS-J Operations

- The GCCS-J v6.0.1.0 OT&E showed that the system was not operationally effective and not operationally suitable. Fifty-five problem reports remained open at the conclusion of OT&E, of which four resulted in complete or partial mission failure with no means to resolve and mitigate the deficiencies. JITC was not able to test 15 of 29 critical interfaces because they were not available at either test site. The system experienced failures on average every 3 hours, much less than the specified requirement. However, the system did demonstrate the ability to perform the majority of its design capabilities.
- Following the GCCS-J v6.0.1.0 OT&E, the C2 ESC determined that the system was not ready for operational use. The C2 ESC directed DISA to field the updated GCCS-J v6.0.1.2, with defect fixes, to multiple Combatant Commands and the JSSC in order to conduct additional testing to validate OT&E fixes and to determine system stability in the operational environment.
- The GCCS-J v6.0.1.2 OA showed that the system is not operationally effective or operationally suitable. Although USCENTCOM and USINDOPACOM validated the Program Office fixed 4 high priority and 17 lower priority defects found during OT&E, users discovered 21 new defects during the OA of which 10 resulted in complete or partial mission failure with no means to resolve or mitigate these deficiencies. DISA should have found many of these defects in developmental testing and resolved them prior to the OA. The OA also showed that GCCS-J v6.0.1.2 is not stable in the operational environment.

GCCS-J Modernization

- GCCS-J Modernization demonstrations for the first three PIs during FY19 showed that development is progressing as planned.
- User feedback from the GCCS-J Modernization limited user assessment was mostly positive; however, users observed

that many capabilities required additional development. Users also identified defects and requested enhancements, which DISA added to the backlog.

- PI 4 will focus on hardening the GCCS-J Modernization system to improve its cybersecurity posture in preparation for an Authority to Operate on the SIPRNET.

JPES

- During the Program Office and JITC-conducted RRE, system administrators installed and sustained the JPES Framework in the operational environment and successfully completed portions of the Continuity of Operations plan. The JPES Framework completed accurate, complete, and timely information exchanges with JOPES, JCRM, and PFG.

Recommendations

DISA should:

1. Resolve GCCS-J v6.0.1.2 Priority 1 and 2 problem reports and correct system stability problems.
2. Operationally test the system at USCENTCOM, USINDOPACOM, USSTRATCOM, and the JSSC prior to sunsetting the currently fielded GCCS-J v4.3.
3. Complete GCCS-J v6.0.1.2 interoperability testing of the remaining critical interfaces at Combatant Command sites.
4. Conduct cybersecurity testing on the operational version of Global v6.0.1.2, in accordance with DOT&E-approved cybersecurity test guidelines.
5. Review the GCCS-J developmental test program and develop options for improving the effectiveness of developmental testing across the C2 portfolio.

FY19 DOD PROGRAMS