

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

## Executive Summary

- In FY20, the Global Command and Control System – Joint (GCCS-J) Program Manager sustained the existing GCCS-J v4.3 baseline and developed GCCS-J Global v6.x. The Joint Planning and Execution Services (JPES) Program Manager sustained the existing Joint Operation Planning and Execution System (JOPES) v4.3 baseline and developed JPES.
- In January 2020, the Defense Information Systems Agency (DISA) halted development of the GCCS-J Enterprise Modernization program after a yearlong effort. Moving forward, DISA plans to evolve technical capabilities and implement an enterprise-centric architecture as part of the GCCS-J v6.x program.

## GCCS-J Global

- The Joint Staff and DISA sunset GCCS-J v4.3 in September 2020 prompted all users to migrate to version 6.x.
- Coronavirus (COVID-19) pandemic restrictions prevented the Joint Interoperability Test Command (JITC) from validating fixes to defects identified during previous operational testing and from determining GCCS-J v6.0.1.11 stability in the operational environment, prior to the GCCS-J v4.3 sunset.
- COVID-19 restrictions also prevented JITC from completing cybersecurity testing of GCCS-J v6.0.1.6 at U.S. Southern Command (USSOUTHCOM), Miami, Florida.

## JPES

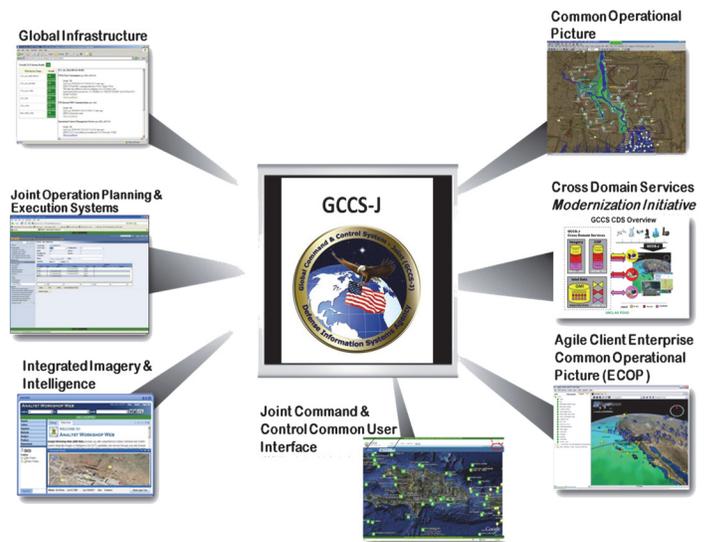
- DISA rebaselined JPES in November 2019. The Program Office plans to use “agile” software processes to develop the system.

## 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 comprises GCCS-J Global and JPES.

## GCCS-J Global

- GCCS-J v6.0.1.11 is intended to provide back-end services, databases, and system administration functions. Agile Client v5.2 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 GCCS-J Global v6.0.1.11, using incremental Maintenance Releases (MRs) to expand capabilities available to the warfighter.



## 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.

## Mission

Joint Commanders use the GCCS-J to accomplish command and control.

## GCCS-J Global

- Commanders use GCCS-J to:
  - Link the National Command Authority to the Joint Task Force, Combatant 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

# FY20 DOD PROGRAMS

## 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
- Software Developers:
  - Northrop Grumman – Arlington, Virginia
  - Leidos – Arlington, Virginia
  - InterImage – Arlington, Virginia
  - CSRA – Falls Church, Virginia

## Major Contractors

- Government Integrator: DISA – Fort Meade, Maryland

## Activity

### GCCS-J Modernization

- In January 2020, DISA halted development of the GCCS-J Enterprise Modernization program after a yearlong effort. Moving forward, DISA plans to evolve technical capabilities and implement an enterprise-centric architecture as part of the GCCS-J v6.x program.

### GCCS-J Global

- The Program Office approved the following releases in FY20:
  - v6.0.1.5 MR in October 2019
  - v6.0.1.6 MR in December 2019
  - v6.0.1.7 MR in February 2020
  - v6.0.1.8 MR in May 2020
  - v6.0.1.9 MR in May 2020
  - v6.0.1.10 MR in June 2020
  - v6.0.1.11 MR in September 2020
  - v6.0.1.12 MR in September 2020
  - v6.0.1.13 MR in November 2020
- JITC conducted a cooperative vulnerability and penetration assessment of GCCS-J v6.0.1.6 at USSOUTHCOM February 5 – 14, 2020. COVID-19 restrictions prevented JITC from completing the adversarial assessment. JITC is planning to complete GCCS-J v6.x cybersecurity testing in 4QFY21.
- JITC conducted a user assessment of the JPES Collaboration Tool (JCT), a component of GCCS-J v6.0.1.11 MR, at 15 sites, August 3 – 18, 2020. DISA developed the JCT to replace the legacy NEWSGROUP capability in GCCS-J v4.3. In accordance with DOT&E policy, this low-risk upgrade warranted a level I operational test, which did not require a DOT&E-approved test plan.
- Following poor results during the user assessment, DISA removed the JCT capability from the GCCS-J v6.0.1.11 MR and extended the GCCS-J Authority to Operate to allow continued use of the GCCS-J v4.3 NEWSGROUP capability.

- The Joint Staff and DISA sunset GCCS-J v4.3 in September 2020 prompting all users to migrate to version 6.0.12.

## JPES

- DISA rebaselined JPES in November 2019. The Program Office plans to use “agile” software processes to develop the system.

## Assessment

### GCCS-J Global

- COVID-19 restrictions prevented JITC from validating OT&E fixes to defects identified during previous operational testing and from determining GCCS-J v6.0.1.11 stability in the operational environment, prior to the GCCS-J v4.3 sunset.
- The JCT user assessment showed that the capability did not support JPEC collaboration. Thirteen problem reports remained open at the conclusion of testing, of which seven resulted in complete or partial mission failure with no means to resolve and mitigate the deficiencies. The DISA developmental test program should have discovered many of these defects prior to the JCT user assessment.

## Recommendations

DISA should:

1. Resolve JCT Priority 1 and 2 problem reports.
2. Operationally test GCCS-J v6.1 at Combatant Command sites to validate Program Office fixes to defects identified during previous operational testing and to determine system stability in the operational environment.
3. Complete cybersecurity testing on the operational version of GCCS-J Global v6.1, in accordance with DOT&E-approved cybersecurity test guidelines.
4. Continue to improve the GCCS-J developmental test program.