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


**The Global Command and Control System - Joint (GCCS-J) family of systems includes Joint Operation Planning and Execution System (JOPES) and Joint Planning and Execution Services (JPES), among other command and control systems. While GCCS-J was reported as not operationally effective in the FY19 DOT&E Annual Report, GCCS-J has demonstrated some progress towards effectiveness in FY22 testing. In FY23, operational effectiveness and operational suitability will be evaluated during the GCCS-J v6.1 FOT&E. GCCS-J and JPES have adopted agile software development methods using development, security, and operations (DevSecOps) processes.**

## SYSTEM DESCRIPTION

GCCS-J is a software-based system with commercial off-the-shelf and government off-the-shelf software and hardware 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. The JPES Program Management Office (PMO) is continuing sustainment of the JOPES v4.5.0.0 until JPES can be deployed to all JOPES users.

## MISSION

The GCCS-J family of systems enables Joint Commanders to accomplish command and control by:

- Linking the National Command Authority to the Joint Task Force, component commanders, and service-unique systems at lower levels of command;
- 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;
- Providing a missile warning and tracking capability;
- Translating policy decisions into operations plans that meet U.S. requirements to employ military forces;
- Supporting force deployment; and
- Conducting contingency and crisis action planning.

## PROGRAM

The GCCS-J PMO intends to field version v6.1.0.0 as an upgrade to the fielded version of v6.0.1 in FY23. The JPES PMO intends to continue development and conduct user assessments to ensure all necessary functionality meets or exceeds that of JOPES, which JPES is replacing. GCCS-J and JPES are implementing the DevSecOps process as part of their agile software development framework.

### » MAJOR CONTRACTORS

**GCCS-J:**

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

**JPES/JOPES:**

- InterImage Inc. – Arlington, Virginia
- ERP International, LLC – Laurel, MD
- NextGen Federal Systems – Morgantown, WV
- CompQSoft – Leesburg, VA

## TEST ADEQUACY

In FY22, the Joint Interoperability Test Command (JITC) conducted two user assessments (UAs) for GCCS-J, two UAs for JPES, and one operational assessment for JOPES, in accordance with DOT&E policy. The GCCS-J and JPES integrated test environments do not currently capture the mission configurations associated with each Combatant Command and other critical sites. GCCS-J and JPES test strategies need to be developed to encompass the agile nature and varying operational site requirements to inform the Test and Evaluation Master Plans (TEMPs) and the Agile Operational Master Test Plans. Additionally, TEMP updates for the GCCS-J and JPES programs should detail operational cyber survivability tests that include cooperative vulnerability and penetration assessments followed by adversarial assessments.

## PERFORMANCE

### » EFFECTIVENESS

In FY19, DOT&E reported that the GCCS-J v6.0.1.0 FOT&E demonstrated that the system was not operationally effective. Based upon the PMO-conducted integration testing and JITC-

conducted UAs in FY22, GCCS-J has demonstrated some progress towards effectiveness. In FY23, operational effectiveness will be evaluated during the GCCS-J v6.1 FOT&E.

JOPES v4.5.0.0 remains operationally effective. JOPES v4.5.0.0 resolved potential end-of-life concerns due to delays in the deployment of JPES.

## » SUITABILITY

In FY19, DOT&E reported that the GCCS-J v6.0.1.0 FOT&E demonstrated that the system was not operationally suitable. During UAs of GCCS-J v6.0.1.x releases, users have reported some improvement in operational suitability. Due to the lack of operational representativeness in the DT environment, suitability will be evaluated during the FY23 GCCS-J v6.1 FOT&E. JOPES v4.5.0.0 remains operationally suitable.

## » SURVIVABILITY

In FY19, DOT&E recommended that cyber survivability testing of GCCS-J v6.0.1.0 should be conducted in accordance with DOT&E cyber survivability policy. Due to delays in the delivery of GCCS-J v6.0.1, operational cyber survivability testing has yet to be conducted. JITC conducted developmental cyber testing of JOPES v4.5.0.0in FY22.

# RECOMMENDATIONS

DISA should:

1. Improve the operational realism, and verify and validate the operational representativeness of the GCCS-J and JPES integrated test environments to ensure testing more closely reflects the diversity of deployment configurations in the operational environment.
2. Revise Agile Operational Master Test Plans and TEMPs for GCCS-J and JPES to reflect agile software development methods, the varied operational site requirements, and operational cyber survivability testing.