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

Executive Summary

- In FY18, the Defense Information Systems Agency (DISA) development of Global Command and Control System – Joint (GCCS-J) focused on the major components of GCCS-J: GCCS-J Global and the Joint Operation Planning and Execution System (JOPES).

Global

- The Program Office used incremental Maintenance Releases (MRs) to develop Global v6.0, completing four Global v6.0 MRs in FY18, which added intelligence, targeting, and chemical/biological/radiological/nuclear defense capabilities to the system. The Joint Interoperability Test Command (JITC) observed and reported on the Global v6.0 MR Level I operational tests. Operational testing in FY18 confirmed that the Program Office implemented the majority of new capabilities and defect fixes successfully. In cases where testers found defects, the Program Office removed the defective capability or component prior to deploying the MR to users.

JOPES

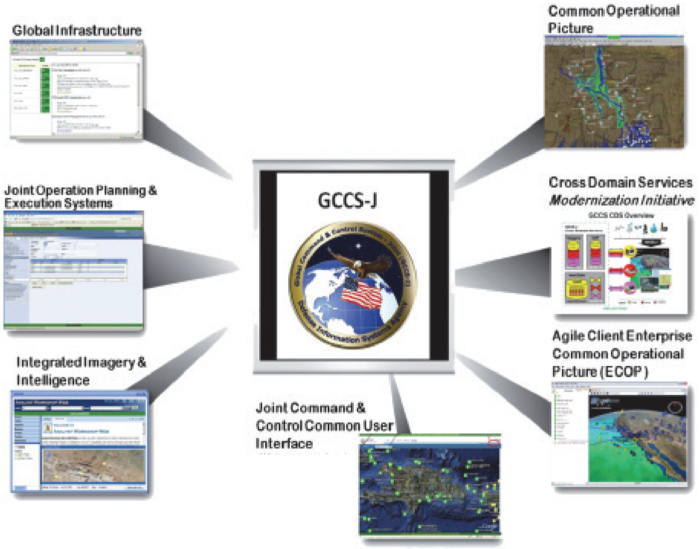
- The Program Office added U.S. Cyber Command (USCYBERCOM) and supporting command Joint Deployment Training Center (JDTC) to the currently fielded JOPES v4.3 using MRs. JITC operationally tested JOPES v4.3.0.1 MR and JOPES v4.3.0.2 MR in FY18, and found them operationally effective and operationally suitable.
- JITC and the DISA Red Team conducted a Cooperative Vulnerability and Penetration Assessment (CVPA) and Adversarial Assessment (AA) of v4.2.0.3 MR4 from January through March 2018. The cybersecurity testing was not adequate for DOT&E to determine JOPES v4.2.0.3 MR4 survivability in a cyber-contested environment. DISA agreed to plan and execute additional cybersecurity testing on JOPES to fully characterize the cyber survivability of 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. Global and JOPES are the two baseline systems that comprise GCCS-J.

Global (Force Protection, Situational Awareness, and Intelligence applications)

- Global v4.3.0.13 is currently fielded worldwide.
- Global v6.0.0.9 and Agile Client v5.2.0.2 are currently fielded at a limited number of sites. DISA is developing Global v6.0.1.0 to replace Global v4.3.0.13.


Global Infrastructure
Common Operational Picture
Joint Operation Planning & Execution Systems
GCCS-J
Cross Domain Services Modernization Initiative
GCCS CDS Overview
Agile Client Enterprise Common Operational Picture (ECOP)
Integrated Imagery & Intelligence
Joint Command & Control Common User Interface

- Global v6.0.1.0 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 v6.0.1.0, releasing incremental MR packages to expand capabilities available to the warfighter.
- DISA is developing GCCS-Joint Enterprise (JE) to replace Global v4.3.0.14, Global v6.0.1.0, and Agile Client Release v5.2.0.2. GCCS-JE is intended to provide situational awareness using a data subscription service, ending the current dependence on a local software instantiation of GCCS-J Global. The Services and Combatant Commands will need to modify their command and control systems to interface with the new GCCS-JE data service.

JOPES (Force Employment, Projection, Planning, and Deployment/Redeployment applications)

- JOPES v4.3.0.2 is the currently fielded version.
- DISA is developing Joint Planning and Execution System (JPES) to replace the JOPES v4.3 baseline. JPES provides all of the functionality of the current JOPES in a modernized architecture.

Mission

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

Global

- Commanders use Global 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 Global to:
  - Build the air picture portion of the common operational picture and maintain its accuracy
  - Correlate or merge raw track data from multiple sources
  - Associate raw electronics intelligence data with track data
  - Perform targeting operations

JOPES

- Commanders use JOPES 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

Global

- The Program Office conducted and JITC observed and reported on the following:
  - Level I operational test of Global v6.0.0.6 MR at the DISA laboratory from November 21 to December 2017
  - Level I operational test of Global v6.0.0.8 MR at the DISA laboratory from March 7 – 12, 2018
  - Level I operational test of Global v4.3.0.12 at the DISA laboratory December 12 – 13, 2017
- The Program Office approved the following releases in FY18:
  - Global v6.0.0.6 MR for release on March 5, 2018
  - Global v6.0.0.7 MR for release on March 12, 2018
  - Global v6.0.0.8 MR for release on April 4, 2018
  - Global v6.0.0.9 MR for release on June 20, 2018
  - Global v4.3.0.13 MR for release on August 28, 2018
  - GCCS-J v5.2.0.2 plug-in on September 10, 2018
- JITC conducted the GCCS-J v6.0.1.0 level II operational test at U.S. Central Command and U.S. Indo-Pacific Command September 17 – 28, 2018, in accordance with a DOT&E-approved test plan.

JOPES

- JITC and the DISA Red Team conducted cybersecurity testing on v4.2.0.3 MR4 remotely from Fort Huachuca, Arizona, and Chambersburg, Pennsylvania. The DISA Red Team failed to conduct the test in accordance with the DOT&E-approved test plan, resulting in an inadequate test. JITC and the DISA Red Team conducted the CVPA, from January 22 through February 1, 2018, and the AA, from February 19 through March 1, 2018, against the primary JOPES server located in the Pentagon, Washington, D.C.
- JITC and the Program Office conducted the following:
  - An operational test of JOPES v4.3.0.1 at the Fort George G. Meade (FGGM) Lab, Maryland, from April 16 through May 2, 2018
  - An operational test of JOPES v4.3.0.2 at the FGGM Lab from August 7 – 10, 2018

Assessment

Global

- The Program Office added functionality to address operational needs in the intelligence, targeting capabilities, and chemical, biological, radiological, and nuclear defense mission areas and corrected 56 defects in Global v6.0.0.6 MR. The release met all but one of the Key Performance Parameters. A new capability, designed to allow the web-based Joint Warning and Reporting Network (JWARN) application to be displayed using Agile Client, failed during testing. Users can still complete their mission using the standard JWARN web display.
- The Program Office added Java Runtime Environment (JRE) 8 to Global v4.3.0.12, replacing non-supported JRE versions in the GCCS-J v4.3 baseline. Testers successfully completed validation of JRE 8 and regression testing of capability areas that could be affected by this upgrade.
- GCCS-J v6.0.1.0 level II operational test results are pending the analysis of collected data.
- JITC is planning to conduct a CVPA and AA of the operational Global v6.0.1.0 at a Combatant Command site in 4QFY19, following system deployment.

JOPES

- JOPES cybersecurity testing in FY18 was not adequate for DOT&E to determine v4.2.0.3 MR4 survivability in a cyber-contested environment. During the AA, the DISA Red Team completed only two of seven planned attacks and did not conduct any advanced attacks. DISA agreed to plan and execute advanced adversarial attacks against JOPES to fully characterize the survivability of the system.
- JOPES v4.3.0.1 is operationally effective and operationally suitable. The Program Office corrected six defects in this

release. Testers discovered one low priority defect with the JOPES v4.3.0.1 software. Users identified an operational workaround for the new defect.

- JOPES v4.3.0.2 is operationally effective and operationally suitable. The Program Office added the USCYBERCOM and supporting command JDTC to the JOPES system, each with its own operation plan series. Operational testing showed that USCYBERCOM and JDTC could create operation plans and force requirements; source, update, and validate force requirements; and schedule and move forces. JITC successfully completed regression testing for 13 of 17 available external interfaces.

Recommendation

1. DISA should conduct a CVPA and AA on the operational version of Global v6.0.1.0, in accordance with DOT&E-approved cybersecurity test guidelines.