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

Executive Summary

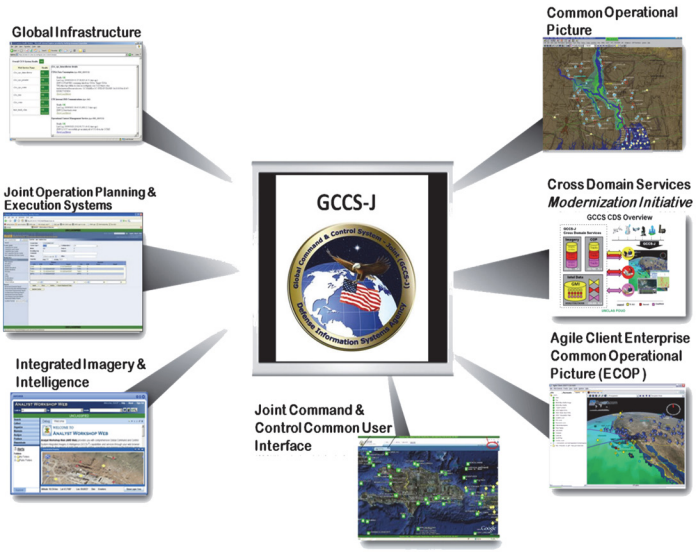
- In FY15, Defense Information Systems Agency (DISA) development of Global Command and Control System – Joint (GCCS-J) focused on fixing cybersecurity vulnerabilities, implementing high-priority capability enhancements, and software defect corrections to both the GCCS-J Global (referred to as Global) and Joint Operation Planning and Execution System (JOPES).

Global

- JITC conducted a Global v5.0 pilot test in January 2015 in preparation for entering operational testing. Global v5.0 failed to satisfy operational test entrance criteria, and DISA, with concurrence of the operational community, subsequently cancelled Global v5.0 in order to reduce risk to Global v4.3 Update 1 sustainment and Global v6.0 development.
- DISA developed Global v4.3 Update 1 Emergency Release 1 to resolve an operational deficiency discovered in the fielded Global v4.3 Update 1 software. This release also included some of the improvements originally planned for the cancelled Global v5.0. The Joint Interoperability Test Command (JITC) and DISA tested Global v4.3 Update 1 Emergency Release 1 in April 2015.
  - GCCS-J Global v4.3 Update 1, with Emergency Release 1, remains effective for use in higher echelons. Testing of Global v4.3 Update 1 for use in lower echelons will occur in FY16 as part of Air Operations Center – Weapons System operational testing.
  - GCCS-J v4.3 is operationally suitable. System installation, help desk, training, and availability are all acceptable.
  - GCCS-J v4.3 Update 1 is not survivable. DISA has not fixed all vulnerabilities identified by the National Security Agency (NSA) cybersecurity testing, and additional vulnerabilities have been identified by cybersecurity testing as part of major Combatant Command exercises.

JOPES

- DISA developed JOPES v4.2.0.3 Emergency Release 4 to implement Global Force Management capabilities and to implement Operational Plan Relevancy codes. JITC conducted an operational test of JOPES v4.2.0.3 Emergency Release 4 in June 2015.
  - JOPES v4.2.0.3 Emergency Release 4 is operationally effective and suitable. Users successfully employed new Global Force Management capabilities and completed all mission tasks.
  - The cyber survivability of JOPES v4.2.0.3 Emergency Release 4 has not yet been tested.



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.
- GCCS-J consists of a client/server architecture using open-systems standards, government-developed military planning software, and, increasingly, use of World Wide Web technology.
- GCCS-J consists of two components, GCCS-J Global and JOPES.

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

- Global v4.3 Update 1, Emergency Release 1 is the currently fielded version. DISA developed Global v4.3 Update 1 to implement high-priority intelligence mission updates to the Theater Ballistic Missile correlation systems, Joint Targeting Toolbox, and Modernized Integrated Database. The update also resolved 49 defects affecting other parts of the system and implemented security lockdown scripts and Information Assurance Vulnerability Alert updates. Emergency Release 1 resolved an operational deficiency discovered in the fielded Global v4.3 Update 1 software.
- Global v5.0. DISA developed Global v5.0 to introduce updates and new features to the Cross-Functional/ Infrastructure, Situational Awareness, and Integrated Imagery and Intelligence mission areas. DISA also fixed 33 problems, all of which had approved operational workarounds. Poor test results in 2015 induced DISA to

cancel Global v5.0 and instead focus on development of Global v6.0.
- Global v6.0. This version will contain features from v5.0 and implement an Agile Client as the primary GCCS-J user interface to allow removal of the global client from the system baseline. DISA is also modernizing Global interfaces to provide greater flexibility for information sharing with external systems.

JOPES (Force Employment, Projection, Planning, and Deployment/Redeployment applications)
- JOPES v4.2.0.3 Emergency Release 4 is the currently fielded version. DISA developed JOPES v4.2.0.3 Emergency Release 4 to implement Global Force Management capabilities and to implement Operational Plan Relevancy codes. Force Tracking Number and Deployment Order information were added to the system, as well as an ability to identify and query operationally relevant plans. DISA also corrected seven critical deficiencies.

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, redeployment, retrograde, and re-posturing
  - Conduct contingency and crisis action planning

Major Contractors
- Government Integrator: Defense Information Systems Agency (DISA)
- Software Developers:
  - Northrop Grumman – Arlington, Virginia
  - Leidos – Arlington, Virginia
  - Pragmatics – Arlington, Virginia

Activity

Global
- In September 2014, DISA approved Global v4.3 Update 1 fielding, based on results from developmental and operational testing conducted in 2014. DISA fixed eight of nine cybersecurity vulnerabilities identified as part of NSA cybersecurity testing shortly after fielding.
- JITC conducted the Global v5.0 pilot test at U.S. Special Operations Command, MacDill AFB, Florida, from January 7 – 9, 2015, to assess the systems readiness to enter operational test. Global v5.0 failed to satisfy operational test entrance criteria, and DISA, with concurrence of the operational community, subsequently cancelled Global v5.0 in order to reduce risk to Global v4.3 Update 1 sustainment and Global v6.0 development.
- DISA developed Global v4.3 Update 1 Emergency Release 1 to resolve an operational deficiency discovered in the fielded Global v4.3 Update 1 software. This release also included some of the improvements originally planned for Global v5.0. In April 2015, JITC and DISA conducted a level 1 operational test of Global v4.3 Update 1 Emergency Release 1 in accordance with a DOT&E-approved policy that did not require a DOT&E-approved test plan.
- On January 7, 2015, the Joint Staff released a memorandum directing a comprehensive review of Global critical and non-critical interface requirements. The Joint Staff directed the review to confirm that Service member data exchange requirements in support of operational missions were being met. This review helped update the correct critical interfaces, and the results of these updates will drive the content, development, and testing of Global v6.0.

JOPES
- In June 2015, JITC conducted a level 1 operational test of JOPES v4.2.0.3 Emergency Release 4 in accordance with a DOT&E-approved policy that did not require a DOT&E-approved test plan. This testing included interface testing with Defense Readiness Reporting System – Strategic.

Assessment

Global
- GCCS-J v4.3 Update 1, with Emergency Release 1, is effective for use in higher echelons.

  - Further operational testing is required to determine the effectiveness for use in lower echelons, such as Air Operations Centers. The interface requirement updates directed by the Joint Staff will assist the Air Operations Center test community in assessing effectiveness at lower echelons.
  - Developmental testing of Global v4.3 Update 1 is planned for the Air Operations Center community in October 2015, with operational testing planned for January 2016.
- GCCS-J Global v4.3 Update 1 is not survivable.
  - DISA has fixed eight of nine significant vulnerabilities identified by NSA cybersecurity testing; however, one significant vulnerability remains. Additional GCCS-J vulnerabilities have been identified by DOT&E-sponsored cybersecurity testing during major Combatant Command exercises.
- GCCS-J v4.3 Update 1 is operationally suitable. System installation, help desk, training, and availability are all acceptable.

JOPES

- JOPES v4.2.0.3 Emergency Release 4 is operationally effective.
  - Users successfully employed new Global Force Management capabilities and completed all mission tasks.
  - All Combatant Commands experienced data exchange failures linked to either initial subscription or interface maintenance. The Joint Staff, in coordination with the Combatant Commands, updated existing standard operating procedures and identified roles and responsibilities to manage the processes.
  - The JOPES program manager resolved all high-priority problem reports, and JITC did not discover any new problems during operational testing.
  - JOPES demonstrated effective end-to-end data exchanges with the new Joint Capabilities Requirements Manager, as well as with Global Combat Support System – Joint and the Deliberate and Crisis Action Planning and Execution Segments.
- JOPES v4.2.0.3 Emergency Release 4 is operationally suitable.
  - System administrators successfully installed and configured the system. The Combatant Commands validated the updated standard operating procedures to support the new Joint Capabilities Requirements Manager to JOPES interface.
  - The system was available throughout the test period, and users did not notice any degradation of performance or usability.
- The cybersecurity of JOPES v4.2.0.3 Emergency Release 4 has not been tested.

Recommendations

- Status of Previous Recommendations. DISA has addressed one of the two previous FY14 recommendations. However, DISA still needs to conduct cybersecurity testing of GCCS Global v4.3 Update 1 in an operational environment to assess protect, detect, react, and recover capabilities.
- FY15 Recommendations. DISA should:
  1. Correct any remaining major cybersecurity vulnerabilities identified either by the NSA assessment of the GCCS-J v4.3 baseline, or during subsequent Combatant Command exercises.
  2. Conduct cybersecurity testing of both GCCS Global v4.3 Update 1 Emergency Release 1 and the JOPES v4.2.0.3 Emergency Release 4 baselines in operational environments, fix any cybersecurity vulnerabilities identified, and conduct appropriate regression testing.