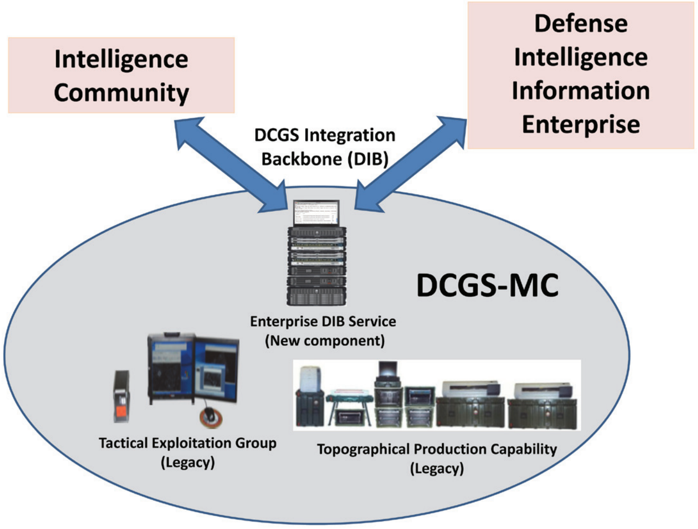
Distributed Common Ground System – Marine Corps (DCGS-MC)

Executive Summary

- The Marine Corps Operational Test and Evaluation Activity conducted the Distributed Common Ground System – Marine Corps (DCGS-MC) IOT&E July 21 – 31, 2014, at Camp Lejeune, North Carolina, in accordance with the DOT&E-approved test plan.
- During IOT&E, DCGS-MC successfully connected to the DCGS Integrated Backbone (DIB), allowing Marines to search and download intelligence from joint and intelligence community users. However, as tested, the DCGS-MC Increment 1 did not enhance the user's ability to produce intelligence products.
- The Marine Corps Information Assurance Red Team discovered significant cybersecurity vulnerabilities during the IOT&E that require correction before fielding. Details are provided in DOT&E's classified IOT&E report.
- The DCGS-MC did not meet availability or reliability requirements and users found the system difficult to use.

System

- DCGS-MC is an Acquisition Category III program. The DCGS-MC is a multi-level secure, integrated family-of-systems. The system is composed of a new Enterprise DIB Service node that delivers web application software on commercial off-the-shelf hardware, integrated with legacy Tactical Exploitation Group and Topographic Production Capability.
- The DCGS-MC provides Marine intelligence analysts access to the DIB. The DIB provides the framework that allows sharing of intelligence services and data via web services. The Army, Navy, Air Force, and intelligence agencies developed and fielded their own versions of DCGS. Via the DIB, intelligence analysts can search for and download intelligence information and post the intelligence product they produce for others to use.


Intelligence Community
Defense Intelligence Information Enterprise
DCGS Integration Backbone (DIB)
DCGS-MC
Enterprise DIB Service (New component)
Tactical Exploitation Group (Legacy)
Topographical Production Capability (Legacy)

Mission

- Marine intelligence analysts will use the DCGS-MC Enterprise system to produce geospatial intelligence products through the processing, exploitation, and analysis of data derived from all Marine Corps organic intelligence sources, nontraditional/battlefield observation/collection of joint, multi-national (coalition/allied) partners in support of Marine Corps operations, and tailored theater and national systems.
- The Marine Air Ground Task Force will use the DCGS-MC to connect intelligence professionals with multi-discipline data sources, analytic assessments, and collection assets via the DIB.

Major Contractors

- Lead System Integrator: Space and Naval Warfare Systems Command (SPAWAR) Systems Center Atlantic – Charleston, South Carolina
- SAIC – Charleston, South Carolina

Activity

- The DCGS-MC Program Office completed four developmental tests between August 2012 and November 2013, followed by a period of fixes and subsequent regression testing through May 2014. The Program Office used the developmental test information to determine that the system was ready to enter operational test.
- The Marine Corps Operational Test and Evaluation Activity conducted the IOT&E from July 21 –31, 2014, at Camp Lejeune, North Carolina, in accordance with the DOT&E-approved test plan. Marine Corps intelligence analysts answered requests for information using operationally representative systems connected to networks providing access to intelligence information. Analysts used the DCGS-MC to search for and download files from the DIB, modify the files, and then upload the modified files back to the DIB.
- In September 2014, the Marine Corps System Command indefinitely postponed the Full Deployment Decision.

Assessment

- During the IOT&E, the intelligence analysts using the DCGS-MC did not demonstrate improved mission performance over the intelligence analysts using the legacy systems. The intelligence analysts using the DCGS-MC answered requests for information (RFIs) with the same quality and response time as the intelligence analysts using the legacy systems. This might be partially attributable to the RFIs not requiring extensive use of external intelligence information. If the Marine Corps implemented updated concept of operations and doctrine to take advantage of the extensive external intelligence available via the DIB, DCGS-MC might show more operational value.
- Marine Corps Information Assurance Red Team adversarial activities and on-site cybersecurity compliance checks and penetration testing identified significant cybersecurity problems that introduce vulnerabilities and reduce the security of the system.
- DCGS-MC did not satisfy availability and reliability requirements, but did satisfy the time to repair requirement.
  - The web-portal on the DIB server froze regularly. The root cause of the problem was not discovered during the developmental test.
  - The DCGS-MC servers were not synchronized to a universal time standard; performance was degraded when drifting occurred.
- Marine Corps intelligence analysts considered the DCGS-MC to be more difficult to use than the current systems. Surveys revealed that they generally preferred the legacy systems.
- On October 31, 2014, DOT&E issued a classified report on the DCGS-MC IOT&E.

Recommendations

- Status of Previous Recommendations. This is the first annual report for this program.
- FY14 Recommendations. The Program Office should:
  1. Correct the cybersecurity vulnerabilities discovered during IOT&E and verify via testing.
  2. Execute a reliability growth program with testing to confirm improvement.
  3. Provide a plan to implement changes to improve system usability that includes verifying improvements using the standard System Usability Scale survey.
  4. Update concept of operations and doctrine to take advantage of external intelligence information available via the DIB.