

Distributed Common Ground System – Navy (DCGS-N)

Executive Summary

- The Commander, Operational Test and Evaluation Force (COTF) conducted an FOT&E of the Distributed Common Ground System – Navy (DCGS-N) Increment 1, Block 2 from August 2015 through January 2016.
- On May 9, 2016, DOT&E reported DCGS-N Increment 1, Block 2 to be operationally effective and suitable, but not survivable against cyber threats to the system.
- The USD(AT&L) approved the DCGS-N Increment 2 Milestone B on September 19, 2016.

System

- DCGS-N is the Navy Service component of the DOD DCGS family of systems, providing multi-Service integration of intelligence, surveillance, reconnaissance, and targeting capabilities.
- DCGS-N Increment 1 uses commercial off-the-shelf (COTS) and mature government off-the-shelf (GOTS) software, tools, and standards. It interoperates with the DCGS family of systems via implementation of the DCGS Integration Backbone and Net-Centric Enterprise Services standards.
- Increment 1 is divided into two blocks: Block 1 delivered initial capability on the legacy ship networks, and Block 2 is a hosted application on the Consolidated Afloat Networks and Enterprise Services (CANES).
- Increment 2 will continue to integrate mature COTS and GOTS services and hardware, but it will be hosted on a cloud computing platform provided by CANES for afloat nodes and maritime operations centers (MOCs).
- Increment 2 will be delivered via five Fleet Capability Releases, vice block releases, using an agile development framework. The key additional capabilities for Increment 2 are: enhanced all-source fusion and analysis to provide better maritime domain awareness; enhanced tasking, collection, processing, exploitation, and dissemination; and enhanced sharing of information across commands, Services, and agencies.



Mission

- The operational commanders use DCGS-N to participate in the Joint Task Force-level targeting and planning processes and to share and provide Navy-organic intelligence, reconnaissance, surveillance, and targeting data to Joint Forces.
- Units equipped with DCGS-N will:
 - Identify, locate, and confirm targets through multi-source intelligence feeds
 - Update enemy track locations and provide situational awareness to the Joint Force Maritime Component Commander by processing data drawn from available sensors

Major Contractor

BAE Systems, Electronics, Intelligence and Support (EI&S) – San Diego, California, and Charleston, South Carolina (for Increment 1 only, Increment 2 contractor is TBD)

Activity

- COTF conducted an FOT&E of DCGS-N Increment 1, Block 2 August 2015 through January 2016 onboard the USS *John C. Stennis*. COTF collected performance data during August through November 2015 and declared the end of test on January 11, 2016, after completing cybersecurity testing. Testing was conducted in accordance with the DOT&E-approved test plan.
- DOT&E submitted a classified memorandum report to the Milestone Decision Authority on the results of the Block 2 test on May 9, 2016.

- The USD(AT&L) approved the DCGS-N Increment 2 Milestone B on September 19, 2016.

Assessment

- DOT&E evaluated the Block 2 system to be operationally effective and suitable, but not survivable against cyber threats to the system.
- Additional details can be found in DOT&E's May 2016 classified report.

FY16 NAVY PROGRAMS

Recommendations

- Status of FY15 Recommendations. The Navy addressed all previous recommendations.
- FY16 Recommendation.
 1. The Navy should remedy cyber vulnerabilities associated with DCGS-N per DOT&E's classified May 2016 report.