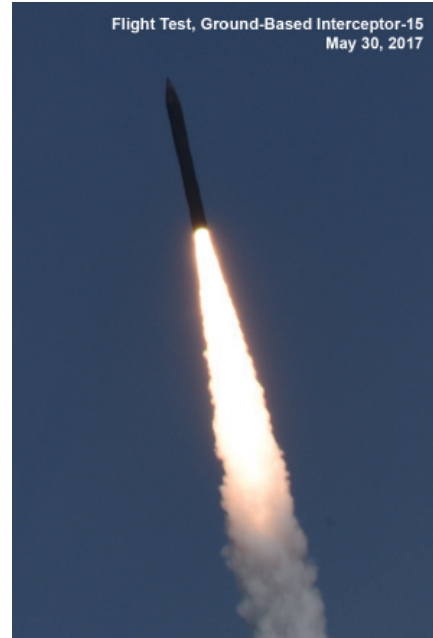


Ground-Based Midcourse Defense (GMD)

Executive Summary

- The Ground-based Midcourse Defense (GMD) element has demonstrated capability to defend the U.S. Homeland from a small number of intermediate-range ballistic missile (IRBM) or intercontinental ballistic missile (ICBM) threats with simple countermeasures when the Homeland Defense Ballistic Missile Defense System (BMDS) employs its full architecture of sensors and command and control.
- The Missile Defense Agency (MDA) declared a BMDS Homeland Defense technical capability of 44 Ground-Based Interceptors (GBIs) in December 2017.
- In FY18, GMD participated in two BMDS hardware-in-the-loop ground tests, and the MDA conducted extensive test planning in preparation for Flight Test, GBI-11 (FTG-11), which is the first GMD element operational test. FTG-11 is currently scheduled for 2QFY19.
- Quantitative evaluation of GMD operational effectiveness is not yet possible due to lack of sufficient ground testing with independently accredited modeling and simulation (M&S). Comprehensive cybersecurity assessments are required to support a GMD survivability assessment.



System

- GMD counters IRBM and ICBM threats to the U.S. Homeland. GMD consists of:
 - GBIs at Fort Greely, Alaska, and Vandenberg AFB, California.
 - GMD ground system, including Ground Fire Control (GFC) nodes, Launch Management System (LMS), and In-Flight Interceptor Communication System Data Terminals.
 - GMD secure data and voice communications system, including long-haul communications using the Defense Satellite Communication System, commercial satellite communications, and fiber-optic cable (both terrestrial and submarine).
 - External interfaces that connect to North American Aerospace Defense/U.S. Northern Command's Command Center; Command and Control, Battle Management, and Communications (C2BMC) system; Space-Based Infrared System; AN/TPY-2 Forward-Based Mode radars in Japan; and Aegis Ballistic Missile Defense ships through C2BMC.

Mission

Military operators from the U.S. Army Space and Missile Defense Command/Army Forces Strategic Command (the Army component to U.S. Strategic Command) will use the GMD system to defend the U.S. Homeland against IRBM and ICBM attacks using GBIs to defeat threat missiles during the midcourse segment of flight.

Major Contractors

- GMD Prime: The Boeing Company, Network and Space Systems – Huntsville, Alabama
- Boost Vehicle: Northrop Grumman Corporation, Innovation Systems – Chandler, Arizona
- Kill Vehicle: Raytheon Company, Missile Systems – Tucson, Arizona
- Fire Control and Communications: Northrop Grumman Corporation, Information Systems – Huntsville, Alabama

Activity

- The MDA conducted all testing in accordance with the DOT&E-approved Integrated Master Test Plan.
- The MDA delivered the 44th GBI in November 2017 and declared a BMDS technical capability for Homeland Defense the following month.
- The MDA did not conduct GMD flight testing in FY18.
- The GMD program conducted a cybersecurity Enhanced Homeland Defense (EHD) Ground Systems (GS) 7A laboratory-based risk reduction assessment in June 2018 to collect packet capture data, validate cybersecurity tools, and conduct penetration activities in preparation for additional pending cybersecurity testing. A second EHD GMD GS 7A

laboratory-based risk reduction assessment followed by the EHD Adversarial Assessment is planned for FY19.

- GMD participated in two BMDS hardware-in-the-loop ground tests:
 - The first ground test in November 2017 used hardware and software representations of the Homeland Defense BMDS, including the full GMD element, sensor architecture, and command and control suite. This test characterized the BMDS Capability Increment 4 functionality and limitations for ICBM threats.
 - The second test in July 2018 added the BMDS Overhead Persistent Infrared Architecture to the Homeland Defense BMDS and assessed the BMDS performance employing new Exo-atmospheric Kill Vehicle (EKV) Knowledge Database capabilities and GS enhancements during strategic and regional/theater scenarios for U.S. Northern Command and U.S. Indo-Pacific Command.
- In January 2018, the MDA Director extended the Development and Sustainment Contract through 2023 to manage overall program risk while achieving the expanded GMD capability called for in the Missile Defeat and Defense Enhancement Budget Amendment.
- The MDA fielded GMD GS 7A.0.0 hardware and software in January 2018 to improve element efficiency and availability. This enhancement integrated the functions of the independent Command Launch Equipment sub-system into the GFC and LMS. The MDA fielded updates to the initial software (version GS 7A.0.1) in June 2018.
- In February 2018, the MDA moved its Developmental Baseline Review (DBR) planning for the Redesigned Kill Vehicle (RKV), which is the follow-on capability to the EKV program, to the GMD Increment 6 program.
- In May 2018, the MDA definitized the RKV development contract per the approved Acquisition Plan with the Boeing Company.
- Throughout FY18, the MDA continued development of enhancements to the Capability Enhancement-I (CE-I) and CE-II EKVs. Updated software for fielding to the CE-I GBIs, and to the CE-II GBIs, is scheduled for FY19.
- The MDA conducted several executive-level reviews in preparation for FTG-11, and is on track for the first operational test of the GMD element in FY19.

Assessment

- Previous DOT&E assessments that GMD has demonstrated capability to defend the U.S. Homeland for a small number of IRBM or ICBM threats with simple countermeasures when the U.S. Homeland Defense BMDS employs its full architecture sensors and command and control remain unchanged.
- While the MDA made some progress during FY18, quantitative evaluation of GMD operational effectiveness requires extensive ground testing with independently accredited M&S that the MDA has not yet done. Also, more comprehensive threat-realistic operational cybersecurity testing (e.g., Adversarial Assessments preceded by Cooperative Vulnerability and Penetration Assessments), is required to support a quantitative GMD survivability assessment.
- Ground test data and resulting assessments are classified (see the classified DOT&E “FY18 Assessment of the BMDS,” to be published in February 2019).

Recommendations

The MDA should:

1. Develop independently accredited M&S to support quantitative evaluation of GMD effectiveness.
2. Develop a comprehensive operational cybersecurity test and evaluation strategy for the GMD architecture; this strategy should be included in the Integrated Master Test Plan and reflect:
 - GMD coordination with Deputy Assistant Secretary of Defense for Developmental Test and Evaluation to implement cybersecurity developmental testing prior to operational testing.
 - Coordination with the Air Force to conduct integrated operational cybersecurity testing of the Upgraded Early Warning Radars and COBRA DANE radar.
 - Plans to address test limitations and mitigate system deficiencies identified in previous cybersecurity assessments.
 - A process for using previous cybersecurity assessment results to inform cyber testing requirements and future engineering cycles.