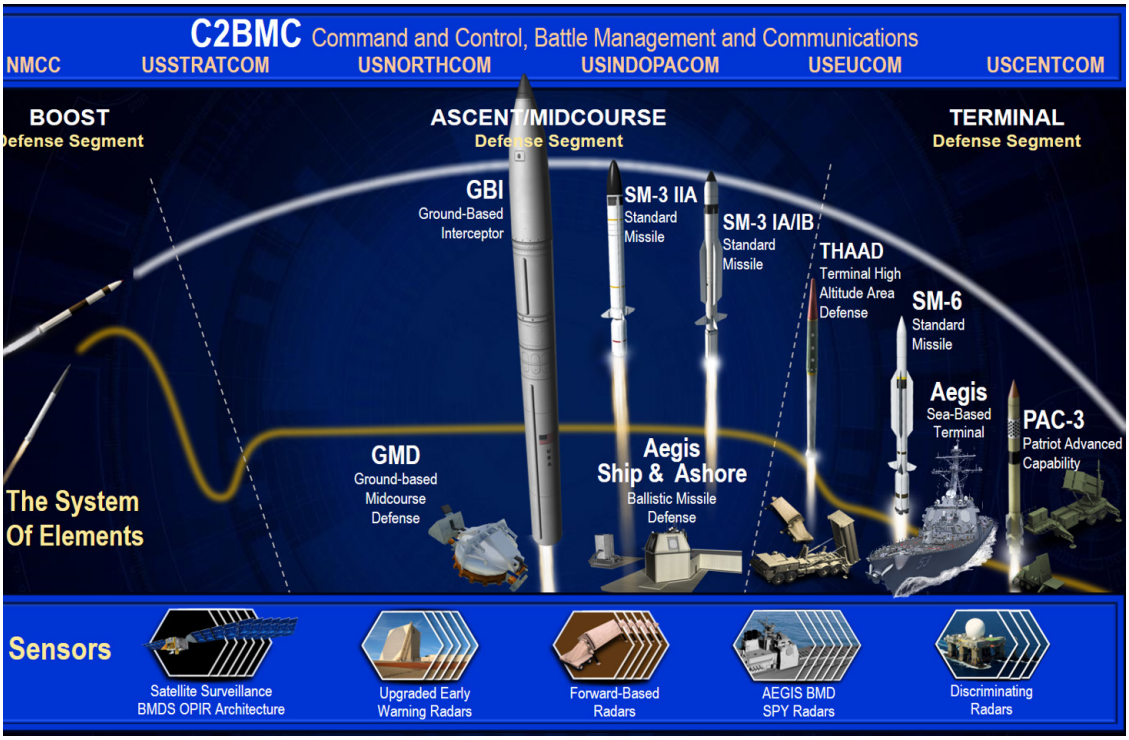
Ballistic Missile Defense System (BMDS)



BMD - Ballistic Missile Defense
BMDS - Ballistic Missile Defense System
NMCC - National Military Comand Center
OPIR - Overhead Persistent Infrared

USCENTCOM - U.S. Central Command
USEUCOM - U.S. European Command
USINDOPACOM - U.S. Indo-Pacific Command
USNORTHCOM - U.S. Northern Command
USSTRATCOM - U.S. Strategic Command

Executive Summary

- The Ground-based Midcourse Defense (GMD) element has demonstrated the capability to defend the U.S. Homeland from a small number of intermediate-range ballistic missile (IRBM) and 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 Regional/Theater BMDS demonstrated a capability to defend the U.S. Indo-Pacific Command (USINDOPACOM), U.S. European Command (USEUCOM), and U.S. Central Command (USCENTCOM) areas of responsibility for small numbers of medium-range ballistic missile and IRBM threats (1,000 to 4,000 km), and a capability for short-range ballistic missile threats (less than 1,000 km range).
- DOT&E assesses the planned Regional/Theater Defense test program as adequate. The Homeland Defense planned test program cannot be assessed due to the strategic pause in the GMD test program. The planned BMDS cybersecurity test program includes sufficient operational testing, but critical developmental testing has not been included in the Integrated Master Test Plan (IMTP).
- The Missile Defense Agency (MDA) continued to mature BMDS operational effectiveness in FY19 during 23 test events. The MDA conducted an additional six international tests and four technology demonstrations. The MDA is making progress characterizing the BMDS cybersecurity posture; however, additional cybersecurity testing is required to support a comprehensive cybersecurity evaluation of the BMDS.
- The MDA continues to resolve limitations that have previously prohibited independent modeling and simulation (M&S) accreditation. Although the MDA still does not have sufficient independently accredited M&S to enable a quantitative evaluation of BMDS operational effectiveness, the models are now adequate for assessing some specific scenarios and functions.

System

The BMDS is a geographically distributed system of systems that relies on element interoperability and warfighter integration for operational capability and efficient use of guided missile/interceptor inventory. The BMDS includes five elements: four interceptor systems and one sensor/command and control architecture.

- Interceptor systems – GMD, Aegis Ballistic Missile Defense (BMD)/Aegis Ashore Missile Defense System, Terminal High-Altitude Area Defense (THAAD), and Patriot.
- Sensor/command and control architecture.
  - Sensors – COBRA DANE radar, Upgraded Early Warning Radars, Sea-Based X-band (SBX) radar, AN/TPY-2 radars (Forward-Based Mode (FBM) and THAAD Mode), Aegis AN/SPY-1 radar aboard Aegis BMD ships, and the Space-Based Infrared System (SBIRS).
  - Command and control – Command and Control, Battle Management, and Communications (C2BMC), including the BMDS Overhead Persistent Infrared Architecture (BOA).

Mission

- The Commanders of U.S. Northern Command (USNORTHCOM), USINDOPACOM, USEUCOM, and

USCENTCOM employ the assets of the BMDS to defend the United States, deployed forces, and allies against ballistic missile threats of all ranges.
- The Commander, U.S. Strategic Command, synchronizes operational-level global missile defense planning and operations support for the DOD.

Major Contractors
- The Boeing Company
  - GMD Integration: Huntsville, Alabama
- Lockheed Martin Corporation
  - Aegis BMD, Aegis Ashore Missile Defense System, and AN/SPY-1 radar: Moorestown, New Jersey
  - C2BMC: Huntsville, Alabama, and Colorado Springs, Colorado
  - SBIRS: Sunnyvale, California
  - THAAD Weapon System and Patriot Advanced Capability-3 Interceptors: Dallas, Texas
  - THAAD Interceptors: Troy, Alabama
  - Patriot Missile Enhancement Segment Interceptors: Dallas, Texas
- Northrop Grumman Corporation
  - GMD Booster Vehicles: Chandler, Arizona
  - GMD Fire Control and Communications: Huntsville, Alabama
  - BOA: Boulder, Colorado; Colorado Springs, Colorado; and Azusa, California
- Raytheon Company
  - GMD Exo-atmospheric Kill Vehicle and Standard Missile (SM)-3/6 Interceptors: Tucson, Arizona
  - Patriot Weapon System including Guidance Enhanced Missile-Tactical interceptors, AN/TPY-2 radar, SBX radar, and Upgraded Early Warning Radars: Tewksbury, Massachusetts
  - COBRA DANE Radar: Dulles, Virginia

Activity
- The MDA conducted testing in accordance with the DOT&E-approved IMTP.
- The MDA, in collaboration with DOT&E, updated the IMTP twice in FY19 to incorporate BMDS element maturation, program modifications, and fiscal constraints.
- The MDA conducted one operational Homeland Defense BMDS test and one element-level operational Regional/Theater Defense Aegis BMD test.
  - Flight Test, GMD Weapon System-11 (FTG-11) in March 2019, was the first two-interceptor salvo engagement of an ICBM target and used data from the SBX radar, the AN/TPY-2 (FBM) radar, C2BMC element, BOA, and SBIRS. The Ground-Based Interceptor (GBI) salvo consisted of a Capability Enhancement-II Block 1 Exo-atmospheric Kill Vehicle on top of a Configuration 2 booster followed by a Capability Enhancement-II Exo-atmospheric Kill Vehicle on top of a Configuration 1 booster.
  - Flight Test, Integrated-03 (FTI-03) was an Aegis BMD engage-on-remote intercept of an air-launched IRBM target using an SM-3 Block IIA missile and based on AN/TPY-2 (FBM) radar data. FTI-03 was the first end-to-end demonstration of Aegis BMD engage-on-remote capability.
  - The MDA conducted 21 additional tests of BMDS weapon systems and sensors/command and control architecture, including 6 cybersecurity assessments. See the individual BMDS element articles (pages 97 and 209-220) for reporting on these tests.
- The MDA continues to resolve limitations that have previously prohibited independent M&S accreditation. In FY19, a joint modeling team was created between the intelligence community and the MDA to resolve long-standing threat modeling problems; the MDA explored new validation techniques for models with little referent data available; and the MDA and BMDS Operational Test Agency Team started addressing emergent modeling requirements.
- The MDA conducted 32 wargames and exercises to enhance Combatant Command BMD readiness and increase Service operator confidence in the deployed elements of the BMDS.

Assessment
- Previous BMDS-level assessments for Homeland and Regional/Theater Defense remain unchanged:
  - GMD has demonstrated capability to defend the U.S. Homeland from a small number of IRBM or ICBM threats with simple countermeasures when the Homeland Defense BMDS employs its full architecture of sensors/command and control.
  - The Regional/Theater BMDS demonstrated a capability to defend the USINDOPACOM, USEUCOM, and USCENTCOM areas of responsibility for small numbers of medium-range ballistic missile and IRBM threats (1,000 to 4,000 km), and a capability for short-range ballistic missile threats (less than 1,000 km range).
- DOT&E assesses the planned Regional/Theater Defense test program as adequate. The planned Homeland Defense test program cannot be assessed due to the strategic pause in the GMD test program. The planned BMDS cybersecurity test program includes sufficient operational testing, but critical developmental testing has not been included in the IMTP.
- In FTG-11, the lead GBI intercepted the ICBM target missile. The trailing GBI intercepted an object per the engagement fire control methodology. The GMD weapon system performed as expected. For additional technical details and lethality results, see the classified DOT&E "FY19 Assessment of the BMDS," to be published in February 2020.
- In FTI-03, an SM-3 Block IIA missile, launched from the Aegis Ashore Missile Defense Test Complex, intercepted

an IRBM target. The Aegis BMD weapon system, C2BMC, and AN/TPY-2 (FBM) radar performed as expected. For additional technical details and lethality results, see the classified DOT&E "FY19 Assessment of the BMDS," to be published in February 2020.

- The MDA continues to make progress characterizing the cybersecurity posture of BMDS Increment 4 and 5 capabilities. Additional operational cybersecurity testing, supplemented by Persistent Cyber Operations, are required to support a comprehensive evaluation of the BMDS network and system cybersecurity and to inform future increment deliveries.
  - All cybersecurity assessments in FY19 identified cybersecurity problems (see the classified DOT&E "FY19 Assessment of the BMDS," to be published in February 2020). Detailed cybersecurity testing for each BMDS element is needed to ensure BMDS cybersecurity problems are found and fixed for current and future BMDS capability increments.
- The number of models accredited has steadily risen over the last 3 years, and the MDA has removed some model limitations and completed studies to quantify the effect of other limitations. While full performance assessments are still not possible, the number of BMDS functions that independently accredited M&S can assess, continues to grow.
  - The BMDS threat set, sensing environments, and communication pathways necessary in the M&S venues are expected to expand in the coming years. The framework and models will require significant updates; modifications; and verification, validation, and accreditation. The pace of ground testing increased in FY19, but was executable largely because models and threats changed very little between tests. The addition of a substantial number of new threats and functionalities will require increased effort to maintain the current pace of testing.

Recommendations

The MDA should:

1. Develop a comprehensive developmental and operational cybersecurity test and evaluation schedule for the BMDS and its various elements. These schedules should be included in the IMTP.
2. Enable Persistent Cyber Operation assessments of BMDS assets in each Combatant Command and of MDA networks and systems to identify and mitigate cybersecurity vulnerabilities of the BMDS posed by realistic cyber threats.
3. Continue to develop independently accredited M&S to enable quantitative evaluation of BMDS operational effectiveness against both current and emerging threats.