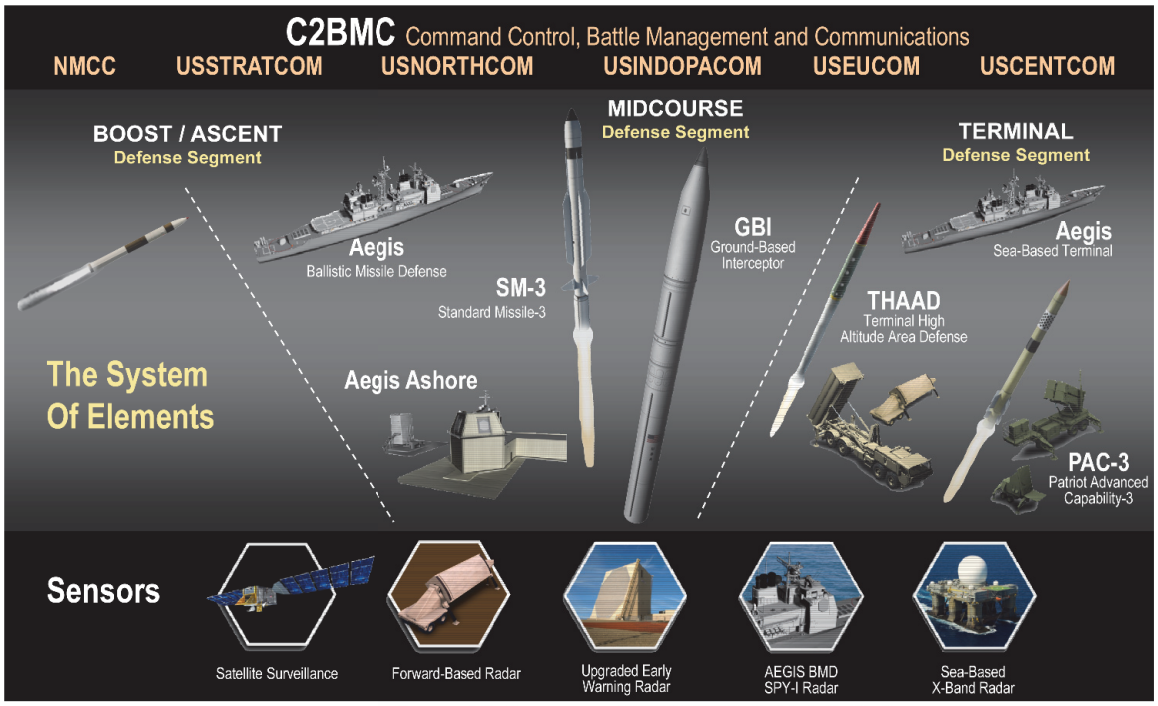
Ballistic Missile Defense System (BMDS)



NMCC – National Military Command Center
USSTRATCOM – U.S. Strategic Command
USNORTHCOM – U.S. Northern Command
USINDOPACOM – U.S. Indo-Pacific Command
USEUCOM – U.S. European Command
USCENTCOM – U.S. Central Command

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) 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).
- The Missile Defense Agency (MDA) has improved its modeling and simulation (M&S) capability over the last 2 years; however, the MDA currently does not have sufficient independently accredited M&S to enable a quantitative evaluation of BMDS operational effectiveness and interoperability.
- Over FY18, the MDA Director emphasized three guiding principles to the agency, enabling significant progress across multiple fronts:
  - Transparency and inclusion of DOT&E, and other interested organizations, in all test meetings from preliminary concept to execution, and at all levels of the MDA.
  - Importance of verification, validation, and independent accreditation of M&S.
  - Improving the cybersecurity posture of BMDS assets by conducting comprehensive, robust cybersecurity assessments and remediation of deficiencies identified in test.

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 combat systems and one sensor/command and control architecture.

- Combat systems – GMD, Aegis Ballistic Missile Defense (BMD)/Aegis Ashore Missile Defense System (AAMDS), Terminal High Altitude Area Defense (THAAD), and Patriot.
- Sensor/command and control architecture.
  - Sensors – COBRA DANE radar, Upgraded Early Warning Radars (UEWRs), Sea-Based X-band (SBX) radar, AN/TPY-2 radars (Forward-Based Mode (FBM) and THAAD Mode (TM)), 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).

FY18 BALLISTIC MISSILE DEFENSE SYSTEMS

Mission
- 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 U.S. Strategic Command (USSTRATCOM) 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, AAMDS, 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-3/6 Interceptors: Tucson, Arizona
  - Patriot Weapon System including Guidance Enhanced Missile-Tactical interceptors, AN/TPY-2 radar, COBRA DANE radar, SBX radar, and UEWRs: Tewksbury, Massachusetts

---

Activity
- The MDA conducted a yearlong test program review resulting in an updated Integrated Master Test Plan (IMTP). DOT&E was included in all planning events and approved the final product.
- During FY18, the MDA did not conduct BMDS-level intercept flight tests, but did execute five element-level intercept flight tests, five ground tests, five cybersecurity Cooperative Vulnerability and Penetration Assessments (CVPAs), three cybersecurity Adversarial Assessments (AAs), two Air Force ICBM reliability and sustainment flight tests, and three individual element data collection flight tests. See the BMDS element articles (pages 205 through 220) for reporting on these tests.
- The MDA conducted numerous wargames and exercises designed to enhance Combatant Command BMD readiness and increase Service member confidence in the deployed elements of the BMDS.
- The MDA initiated development of a BMDS-wide Hypersonic Defense program, which includes near-term capability upgrades, technology development, test planning, and demonstrations over the next several years.
- The MDA conducted CVPAs for the following BMDS assets:
  - X-band radar (XBR) portion of the SBX sensor in October 2017 (limited CVPA).
  - USCENTCOM AN/TPY-2 (FBM) in January 2018.
  - THAAD 3.0 (including the AN/TPY-2 (TM) radar) in March 2018.
  - USEUCOM C2BMC S8.2-3 and BOA 6.1 in July 2018.
  - USEUCOM AN/TPY-2 (FBM) radar in September 2018.
- The MDA conducted the agency's first AAs in FY18: USEUCOM C2BMC S6.4 in March 2018, THAAD 3.0 (including the AN/TPY-2 (TM) radar) at White Sands Missile Range, New Mexico, in April 2018, USEUCOM C2BMC S8.2-3 in September 2018, BOA 6.1 in September 2018, and USEUCOM AN/TPY-2 (FBM) in September 2018.
- In FY18, the MDA established standing ground rules to enable future Persistent Cyber Operations.
- The MDA continues to pursue and resource efforts to resolve major limitations that have prohibited independent M&S accreditation in the past.

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 and command and control.
  - The Regional/Theater BMDS demonstrated a capability to defend the USINDOPACOM, USEUCOM, and USCENTCOM areas of responsibility for small numbers of MRBM and IRBM threats (1,000 to 4,000 km), and a capability for short-range ballistic missile threats (less than 1,000 km range).
- The process used by the MDA to update the IMTP during FY18 was rigorous, transparent, and inclusive of all MDA-internal and DOD-external stakeholders. It produced the most technically comprehensive and DOD-wide coordinated IMTP to date. It is traceable to MDA program priorities, which are:
  - Focus on increasing system reliability to build warfighter confidence.

  - Increase engagement capability and capacity.
  - Rapidly address the advanced threat.
- The MDA continues to make progress characterizing the cybersecurity posture of fielded and soon-to-be fielded BMDS Increment 4 and 5 capabilities. Additional CVPAs and AAs are required to support a comprehensive cybersecurity assessment of BMDS network and system cybersecurity and to inform future increment deliveries.
  - All cybersecurity assessments in FY18 identified cybersecurity findings (see the classified DOT&E "FY18 Assessment of the BMDS," to be published in February 2019). The MDA began to implement more structured cybersecurity test planning activities, and addressed some of the FY17 assessment shortfalls. More deliberate and detailed planning per element is needed to enable strategic cybersecurity assessments across both developmental and operational testing and to ensure findings are applied to future engineering cycles.
  - AAs in FY18 identified ways to improve THAAD, C2BMC, BOA, and AN/TPY-2 (FBM) network defense operations and capabilities in a cyber-contested environment. The GMD program has not yet conducted an AA.
  - The MDA improved upon identifying limitations in advance of testing and should work to implement mitigation strategies for deficiencies identified in FY18 assessments.
- The number of M&S accredited has steadily risen over the last 2 years. While full performance assessments are still not possible, the functional aspects of BMDS performance that can be assessed with independently accredited M&S continue to grow. Concurrently, the MDA is redesigning the process for conducting ground tests with the intent to respond more quickly to Combatant Command needs and evolving threats. While the traditional process does not ensure adequate time for independent M&S verification, validation, and accreditation (VV&A), the MDA is working with OTA to develop VV&A methodologies and data sources to support accreditation.

Recommendations

The MDA should:

1. Continue to use the IMTP update process initiated during FY18.
2. Address findings from cybersecurity assessments.
3. Enable Persistent Cyber Operation assessments of BMDS assets in each Combatant Command and of MDA networks and systems.
4. Integrate DT&E into all cybersecurity assessment planning, to enable discovery and remediation of cybersecurity findings prior to OT&E.
5. Design ground test schedules to account for accreditation timelines. If the ground test results are critical to making technical baseline and fielding decisions, the selection of such decision dates should also consider the availability of accredited models to perform the assessment.