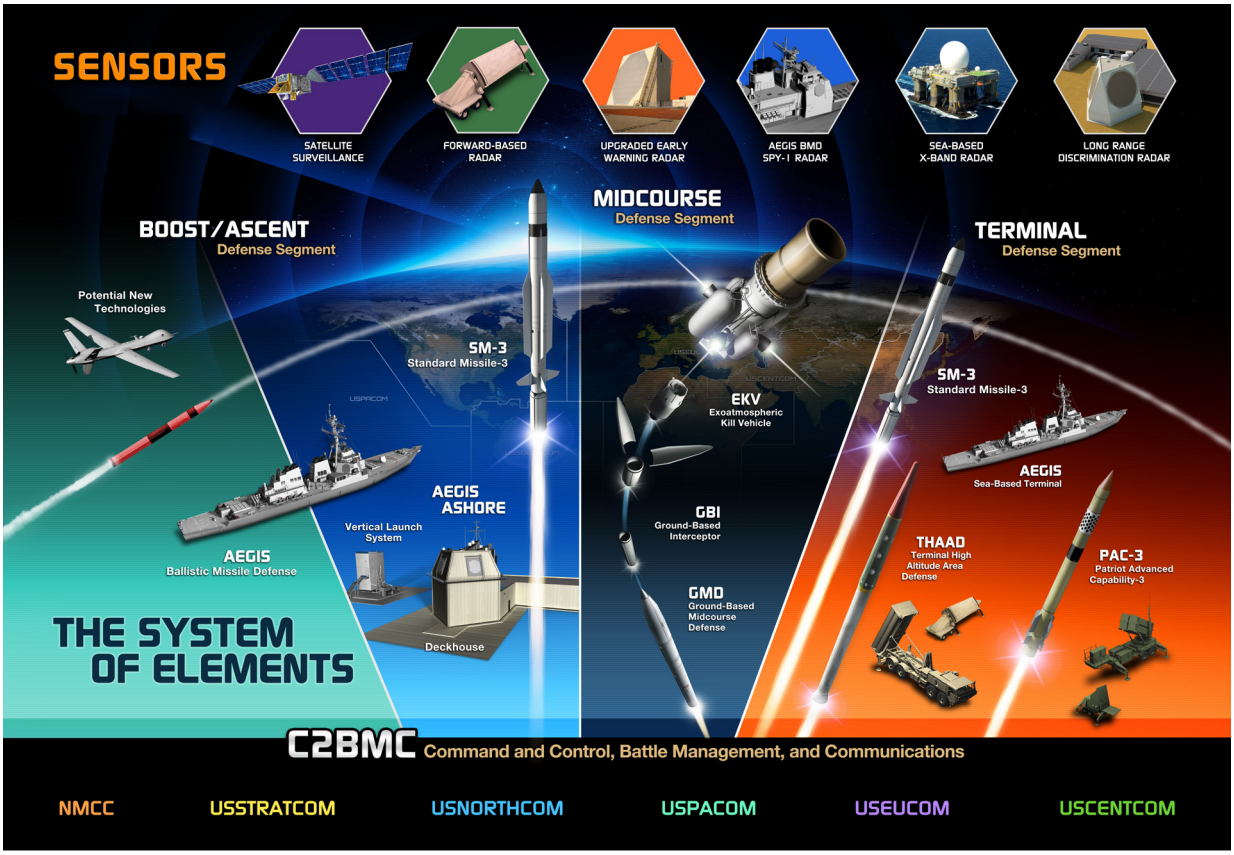
Ballistic Missile Defense System (BMDS)



NMCC - National Military Comand Center
USCENTCOM - U.S. Central Command
USEUCOM - U.S. European Command
USNORTHCOM - U.S. Northern Command
USPACOM - U.S. Pacific Command
USSTRATCOM - U.S. Strategic Command

Executive Summary

- The Ground-based Midcourse Defense (GMD) element demonstrated the 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 sensors/command and control architecture. This assessment is upgraded from FY16.
- The Regional/Theater BMDS demonstrated a limited capability to defend the U.S. Pacific Command (USPACOM), 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 fair capability for short-range ballistic missile threats (less than 1,000 km range). This assessment is unchanged from FY16.
- The Missile Defense Agency (MDA) FY17 cybersecurity assessment activity represents progress and an initial commitment to operational cybersecurity assessment across multiple BMDS elements. The Army Research Laboratory Survivability/Lethality Analysis Directorate conducted cybersecurity assessments on parts of GMD; Command and Control, Battle Management, and Communications (C2BMC); BMDS Overhead Persistent Infrared Architecture (BOA); AN/TPY-2 Forward-Based Mode (FBM) radar; and Sea-Based X-band (SBX) radar. The Cybersecurity Vulnerability and Penetration Assessments (CVPAs) identified cybersecurity vulnerabilities; however, additional, less restrictive testing is required to inform cybersecurity vulnerability mitigation efforts, improve net defense, and characterize BMDS capability in a cyber-contested environment.
- The MDA conducted Flight Test, Ground-Based Interceptor-15 (FTG-15), intercepting an ICBM class target for the first time. FTG-15 was also the first intercept using the Capability Enhancement-II (CE-II) Block 1 exo-atmospheric kill vehicle (EKV) and the first demonstration of the three-stage Configuration 2 booster. The Homeland Defense BMDS performed nominally.
- The MDA conducted nine element-level flight tests and one Navy fleet exercise. No Theater/Regional BMDS-level intercept flight tests took place in FY17.

- The MDA conducted Ground Test, Integrated-07a (GTI-07a) and Ground Test, Distributed (GTD-07a), using strategic and theater/regional scenarios from the U.S. Northern Command (USNORTHCOM) and USPACOM areas of responsibility.
- Since FY10, DOT&E has assessed and reported annually that the lack of independent accreditation of modeling and simulation for performance assessment has limited DOT&E use of these data for quantitative evaluations. This assessment remains unchanged for FY17, although the MDA has made progress in defining high-priority accreditation gaps and allocating resources to address them. The MDA should increase the development priority and ensure adequate funding for the BMDS simulation-based performance assessment capability. This capability should include modeling and simulation verification, validation, and accreditation, as well as the ability to produce high-fidelity and statistically significant BMDS-level performance assessments.
- The MDA conducted numerous wargames and exercises designed to enhance Combatant Command ballistic missile defense (BMD) readiness and increase Service member confidence in the deployed elements of the BMDS.

System

The BMDS is a federated and 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 autonomous combat systems and one sensor/command and control architecture.

- Autonomous combat systems – GMD, Aegis 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), SBX radar, AN/TPY-2 (FBM) radar, Aegis AN/SPY-1 radar aboard an Aegis BMD ship, and the Space Based Infrared System (SBIRS)
  - Command and control – C2BMC, including BOA

Mission

- USNORTHCOM, USPACOM, 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 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
- Northrop Grumman Corporation
  - GMD Fire Control and Communications: Huntsville, Alabama
  - BOA: Boulder, Colorado; Colorado Springs, Colorado; and Azusa, California
- Orbital ATK
  - GMD Booster Vehicles: Chandler, Arizona
- Raytheon Company
  - GMD EKV 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 all testing in accordance with the DOT&E-approved Integrated Master Test Plan (IMTP).
- One developmental homeland defense intercept flight test, FTG-15, occurred in FY17. The MDA conducted FTG-15 in May 2017, intercepting an ICBM-class target for the first time using the GMD system, the AN/TPY-2 (FBM) radar, the C2BMC system, the SBX radar, and the SBIRS. FTG-15 was also the first intercept using the CE II Block 1 EKV and the first demonstration of the three-stage Configuration 2 booster.
- The MDA conducted nine element-level fight tests (five Aegis BMD tests, two THAAD tests, and two Patriot tests) and one Navy fleet exercise. No theater/regional BMDS-level intercept flight tests took place in FY17; the MDA had planned such a test with Aegis BMD and Patriot, however the Navy redirected the Aegis ship to support real-world operations.
- The MDA conducted GTI-07a in June 2017, assessing the BMDS Capability Increment 4 functionality improvements using strategic and theater/regional scenarios from USNORTHCOM's and USPACOM's areas of responsibility.
- The MDA conducted GTD-07a in September and October 2017. It complimented and executed many of the same scenarios as GTI-07a, but in a distributed test environment. GTD ground tests use live operational networks, whereas GTI ground tests use laboratory-based networks.
- 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 conducted cooperative cybersecurity assessments of parts of the following BMDS assets:
  - A limited CVPA of the FTG-15 GMD flight test architecture in June 2017.
  - A CVPA of USNORTHCOM's C2BMC S8.2-1.1, the C2BMC portion of the Cheyenne Mountain Management Node, the C2BMC Distributed Training System, and BOA 5.1 in July 2017.
  - An additional limited cooperative cybersecurity test on USNORTHCOM's C2BMC S8.2-1.1, BOA 5.1, and the AN/TPY-2 (FBM) radar CX2.1.1 configured with the Superdome computer processor in September 2017. The MDA used the event to verify corrective actions for some of the deficiencies identified during the C2BMC S8.2-1 and BOA 5.1 platform CVPA in July 2017.
  - A limited CVPA of the X-band radar (XBR) component of the SBX sensor in October 2017.

Assessment
- 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 sensors/command and control architecture.
- The Regional/Theater BMDS demonstrated a limited capability to defend the USPACOM, 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 fair capability for short-range ballistic missile threats (less than 1,000 km range). The Theater/Regional BMDS assessment remains unchanged since no Theater/Regional BMDS-level intercept flight tests took place in FY17. This also means that there were no flight test opportunities for BMDS-level integrated training for warfighters.
- The MDA made progress toward characterizing the cybersecurity posture of fielded and soon-to-be fielded BMDS Increment 4 capabilities. Additional CVPAs and Adversarial Assessments (AAs) are required to support a comprehensive cybersecurity assessment of BMDS network and system cybersecurity.
  - All CVPAs and cybersecurity assessments in FY17 identified cybersecurity vulnerabilities; however, critical limitations affecting test adequacy resulted from constrained test boundaries; insufficient time to plan, coordinate activity, and resolve technical issues prior to test events; and in the case of AN/TPY-2(FBM) radar, limited asset availability resulting from real-world operational needs in USPACOM.
  - The MDA has not yet conducted any AAs on any operational systems in the BMDS architecture, which are necessary to support a cybersecurity survivability assessment.
- During FTG-15, the Homeland Defense BMDS performed without fault. The three-stage Configuration 2 GBI booster flew as designed and delivered the EKV to the proper geographic position with the desired velocity. The CE-II Block 1 EKV intercepted and negated the ICBM-representative reentry vehicle. Guidance systems throughout the engagement functioned nominally.
- During FY17 ground testing, the MDA exercised new capabilities and assessed BMDS interoperability using hardware-in-the-loop simulation and operational assets communicating over operational networks (GTI-07a and GTD-07a, respectively). Test data informed enhanced homeland defense and theater/regional functionality development for BMDS Capability Increment 4, which is defined as:
  - BOA data integrated into the BMDS and providing X-band cues.
  - BMD planning, SBIRS interface change, and communications enhancements.
  - Performance improvements and GBI reliability upgrade.
  - Implementation of updated cybersecurity protections.
- In FY10, DOT&E reported, "the MDA began execution of its revamped IMTP to collect the data needed to accredit the models and simulations used for assessing performance and effectiveness of the BMDS." Through FY16, DOT&E has assessed and reported annually that the lack of independent accreditation of modeling and simulation for performance assessment have limited DOT&E use of these data for quantitative evaluations. This assessment remains for FY17, although this year the MDA and the BMDS Operational Test Agency jointly identified and are developing plans to resolve the major limitations that have been prohibiting accreditation of the models. Accreditation across the elements and the BMDS framework is still several years away.

Recommendations
- Status of Previous Recommendations. The MDA has addressed all but eight previous BMDS recommendations, three of which are classified and therefore not listed here.
  1. All Services should develop and implement integrated BMDS-level training in formal warfighter certification plans.
  2. Discrimination and debris mitigation techniques warrant further development by MDA.
  3. The MDA should publish a comprehensive BMDS cybersecurity description document that delineates the strategy at the BMDS-level as well as at the element-level for effective cybersecurity, achievable milestones for implementing the strategy, and stakeholder roles and responsibilities at all cybersecurity tiers.
  4. The MDA should conduct comprehensive cybersecurity assessments and electronic warfare testing across all BMDS elements.
  5. The MDA should increase the development priority and associated funding for the BMDS simulation-based

performance assessment capability including modeling and simulation verification, validation, and accreditation, and the ability to produce high-fidelity and statistically-significant BMDS-level performance assessments.

- FY17 Recommendations. The MDA should:
  1. Fund each of the individual elements/model developers to address the major modeling and simulation limitations that are preventing independent accreditation.
  2. Conduct more rigorous operational assessment of BMDS assets via operational CVPAs and AAs to inform cybersecurity vulnerability mitigation efforts, improve net defense, and characterize BMDS capability in a cyber-contested environment. The MDA should leverage opportunities to conduct AAs on operational assets in FY18 in cooperation with ongoing Persistent Cyber Operations and the DOT&E Cybersecurity Assessment Program.
  3. Develop a comprehensive cybersecurity test and evaluation strategy for each BMDS element and implement these strategies through the IMTP. The strategy for each element should include:
     - Plans to conduct independent cybersecurity assessments of existing operational BMDS assets to inform the Department's understanding of the current BMDS cybersecurity posture and operational environment.
     - Cybersecurity test activities earlier in the development cycle to inform system design and software configuration changes.
     - Rigorous operational cybersecurity T&E to support fielding of new capabilities in order to properly inform operational risk assessments; mitigate critical cybersecurity vulnerabilities; improve network defense; and ultimately make BMDS systems and networks more secure against cyber adversaries.
     - Consistent cybersecurity assessment approach, commitment, and accesses to critical BMDS assets across the elements.
  4. In planning cybersecurity events, include sufficient time for the Program Office, the BMDS Operational Test Agency, and DOT&E to obtain needed resources for each event. Late execution of test planning and test plan delivery leaves insufficient time to resolve key issues (e.g., inadequate detail in the test conduct, data management, analysis, and evaluation plans).
  5. Leverage and coordinate with ongoing cybersecurity assessment efforts to conduct operational cybersecurity assessments (CVPAs and AAs) in order to maximize efficiency and reduce duplication of activity across the DOD. These efforts include the DOT&E Cybersecurity Assessment Program, the USD(AT&L) cyber assessment efforts in support of section 1647 of the FY16 National Defense Authorization Act, and the Department's ongoing Persistent Cyber Operations.