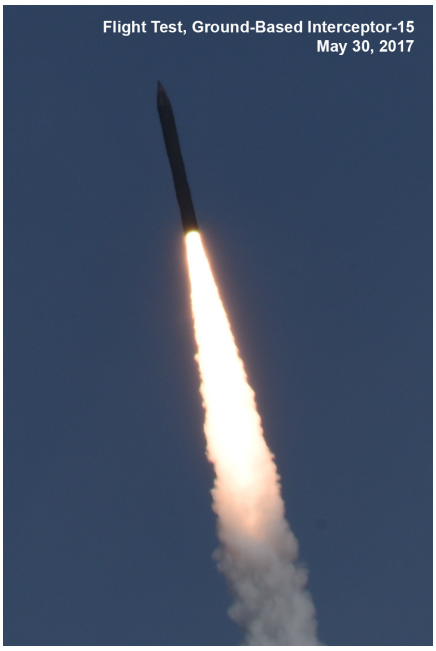
# Ground-Based Midcourse Defense (GMD)

## 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 sensors/command and control architecture.
- The Missile Defense Agency (MDA) intercepted an ICBM-class target for the first time during Flight Test, Ground-Based Interceptor-15 (FTG-15). 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 GMD element performed nominally.
- The Army Research Laboratory Survivability/Lethality Analysis Directorate (ARL/SLAD) conducted a limited Cooperative Vulnerability and Penetration Assessment (CVPA) to assess the cybersecurity of the FTG-15 GMD test architecture. Although testing identified some cyber vulnerabilities, the minimal test scope and the test conduct restrictions prevented an assessment of the overall cybersecurity posture of GMD assets. The MDA has not conducted Adversarial Assessments (AAs) on any GMD systems in the BMDS architecture, which are necessary to support a cybersecurity survivability assessment.
- Quantitative evaluation of GMD operational effectiveness (including system performance, reliability, and lethality) requires extensive ground testing with independently accredited modeling and simulation (M&S), which the MDA has not yet conducted.
- The MDA:
  - Fielded updated GMD Fire Control (GFC) and EKV software.
  - Refurbished Missile Field 1 at Fort Greely, Alaska.
  - Completed the Redesigned Kill Vehicle (RKV) Preliminary Design Review.
  - Emplaced five CE-II Block 1 EKVs with three-stage Configuration 2 boosters, and plans to emplace three more by the end of 2017.
- 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 U.S. Pacific Command (USPACOM) areas of responsibility.

## System

- GMD counters IRBM and ICBM threats to the U.S. Homeland. GMD consists of:
  - Ground-Based Interceptors (GBIs) at Fort Greely, Alaska, and Vandenberg AFB, California.




  - GMD ground system, including GFC nodes at Schriever AFB, Colorado, and Fort Greely, Alaska; Command Launch Equipment at Vandenberg AFB, California, and Fort Greely, Alaska; and In-Flight Interceptor Communication System Data Terminals at Vandenberg AFB, California; Fort Greely, Alaska; Eareckson Air Station, Alaska; and Fort Drum, New York.
  - 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 Aegis Ballistic Missile Defense ships; North American Aerospace Defense/USNORTHCOM Command Center; Command and Control, Battle Management, and Communications system at Schriever AFB, Colorado, and Joint Base Pearl Harbor-Hickman, Hawaii; Space Based Infrared System at Buckley AFB, Colorado; and AN/TPY-2 Forward-Based Mode radars at Japan Air Self Defense Force bases in Shariki and Kyoga-Misaki, Japan.

## 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 the GBI 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: Orbital ATK, Missile Defense 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 fielded GFC 6B3.1 software in January 2017 to mitigate obsolescence and to enhance cybersecurity.
- The MDA fielded CE-II EKV software version 10 to the operational baseline in March 2017.
- The MDA completed the RKV Preliminary Design Review in March 2017.
- The MDA conducted FTG-15 in May 2017, intercepting an ICBM-class target for the first time. 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 GTI-07a in June 2017, assessing the BMDS Capability Increment 4 functionality improvements using strategic and theater/regional scenarios from the USNORTHCOM and USPACOM areas of responsibility.
- ARL/SLAD, in support of the MDA, conducted a limited CVPA of the GMD FTG-15 test architecture in June 2017.
- The MDA completed the refurbishment of Missile Field 1 at Fort Greely, Alaska, in September 2017.
- The MDA conducted GTD-07a in September and October 2017. It 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.
- As of the end of FY17, the MDA has emplaced five CE-II Block 1 EKVs with three-stage Configuration 2 boosters with plans to emplace three more by the end of calendar year 2017.
- The MDA conducted minimal RKV lethality activities in FY17 due to a $55 Million mid-year congressional budget reduction to the RKV program. The MDA reduced the RKV lethality effort by $8.15 Million (94 percent). Test planning and design efforts for light gas gun and/or sled tests were suspended.

**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.
- During FTG-15, the GMD element 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.
- The limited CVPA conducted by ARL/SLAD was a notable first attempt at an independent cybersecurity assessment. Though the assessment identified vulnerabilities, the test was insufficient to inform a cybersecurity evaluation for the operational GMD system. The MDA restricted the assessment to only portions of the GMD architecture associated with FTG-15 located at the Missile Defense Integration and Operations Center at Schriever AFB, Colorado, and Vandenberg AFB, California. The assessment did not include the entire operational environment.
  - The tested components were intentionally isolated from four GMD sites, nine supporting sensors, and the GBI silos and boosters/EKVs.
  - ARL/SLAD could not complete the outsider assessment in accordance with the CVPA test plan due to Temporary Design Departure (TDD) requirements.
  - Within the FTG-15 architecture, the MDA "blacklisted" (i.e., denied access to) critical parts of GMD networks and systems at all locations, limiting an end-to-end assessment. DOT&E and ARL/SLAD were unaware of the blacklist until the start of testing. To mitigate this problem in other FY17 CVPAs, the MDA began to include blacklists as part of the test plans.
  - The MDA did not provide ARL/SLAD and DOT&E sufficient system and network documentation to adequately plan and prepare for the assessment.
- The MDA has not yet conducted a cybersecurity AA of GMD.
- During FY17 ground testing, the MDA exercised new capabilities and assessed BMDS interoperability using hardware-in-the-loop simulation in GTI-07a and operational assets communicating over operational networks in GTD-07a. Test data informed enhanced homeland defense and theater/regional functionality development for BMDS Capability Increment 4, which is defined as:
  - BMDS Overhead Persistent Infrared Architecture data integrated into the BMDS and providing X-band cues.
  - Ballistic missile defense planning, Space Based Infrared System interface change, and communications enhancements.
  - Performance improvements and GBI reliability upgrade.
  - Implementation of updated cybersecurity protections.
- While the MDA made some progress during FY17, quantitative evaluation of GMD operational effectiveness requires extensive ground testing with independently accredited M&S, which the MDA has yet to perform. Due to the lack of required data, the MDA lacks independently

accredited M&S to support an assessment of GMD performance, reliability, and lethality.

**Recommendations**

- Status of Previous Recommendations. The MDA has addressed previous GMD recommendations with the exception of three recommendations, one of which is classified. The MDA should:
  1. Increase emphasis on GMD survivability testing, including cybersecurity. The MDA should plan tests, demonstrations, and exercises to acquire additional survivability data and include them in the BMDS Integrated Master Test Plan.
  2. Accelerate efforts to accredit M&S for performance assessment supporting GMD OT&E, including RKV and countermeasure performance.
- FY17 Recommendation. The MDA should:
  1. Provide adequate funding for and accelerate development of a lethality T&E strategy for the RKV against updated threats and engagement conditions to support performance assessments and M&S tool accreditation.
  2. Develop a comprehensive operational cybersecurity test and evaluation strategy for GMD assets in the BMDS architecture. This strategy should be included in the Integrated Master Test Plan and reflect the following:
     - Planned CVPAs and AAs of existing operational GMD assets and of new increment capabilities, in order to properly inform operational risk assessments; mitigate critical cybersecurity vulnerabilities; improve network defense; and make BMDS systems and networks more secure against cyber adversaries.
     - Elimination of previous practices of port isolation, blacklisting, and restricting assessments for CVPAs and AAs of GMD assets. Discontinuing these practices will enable an adequate evaluation of GMD cybersecurity posture.
     - Sufficient time to plan cybersecurity events, to ensure required resources are available to support adequate test conduct and enable timely resolution of key issues (e.g., inadequate detail in the test conduct, data management, analysis, and evaluation plans).
  3. 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 Department's ongoing Persistent Cyber Operations, and the USD(AT&L) cybersecurity assessment efforts required by section 1647 of the National Defense Authorization Act for FY16.