ATP 3-27.3

Ground-based Midcourse Defense Operations

OCTOBER 2019

DISTRIBUTION RESTRICTION: Approved for public release; distribution is unlimited.

This document supersedes ATP 3-27.3, dated 20 April 2016.

Headquarters Department of the Army

This page intentionally left blank.

This publication is available at the Army Publishing Directorate site (https://armypubs.army.mil), and the Central Army Registry site (https://atiam.train.army.mil/catalog/dashboard)

This page intentionally left blank.

*ATP 3-27.3

Army Techniques Publication
No. 3-27.3

Headquarters
Department of the Army
Washington, DC, 30 October 2019

Ground-based Midcourse Defense Operations

Contents

Page

PREFACE ..... **iv**

INTRODUCTION ..... **v**

Chapter 1 GROUND-BASED MIDCOURSE DEFENSE OVERVIEW **1-1**

Section I – Global Ballistic Missile Defense Overview **1-1**

Army Global Ballistic Missile Defense Mission 1-1

Ballistic Missile Defense System 1-2

Section II – Ground-based Midcourse Defense Overview **1-3**

Mission 1-3

Description 1-3

Ground-based Midcourse Defense Contributing Organizations 1-5

Chapter 2 COMPONENTS **2-1**

Section I – Ground-based Midcourse Defense Ground System **2-1**

Ground-based Midcourse Defense Fire Control 2-1

Launch Support System 2-3

In-Flight Interceptor Communications System 2-4

Section II – Ground-Based Interceptor **2-4**

Orbital Boost Vehicle 2-5

Exo-Atmospheric Kill Vehicle 2-5

Section III – Contributing Sensors and Elements **2-6**

Space Domain 2-6

Land Domain 2-7

Maritime Domain 2-10

Command And Control, Battle Management, And Communications 2-12

Chapter 3 COMMAND AND CONTROL AND SUPPORTING RELATIONSHIPS **3-1**

Command and Control 3-1

Ground-based Midcourse Defense Command and Control Systems 3-2

Titles 10 And 32 United States Code Authorities 3-2

Combatant Commands 3-4

Organizational Structure 3-6

This document supersedes ATP 3-27.3, dated 20 April 2016.

Chapter 4 FIRE CONTROL OPERATIONS 4-1
Section I – Ground-based Midcourse Defense Engagement Operations ... 4-1
Operations Planning 4-1
Engagement Criteria 4-1
Engagement Operations 4-2
Readiness Condition 4-5
Section II – Techniques 4-5
Employment Guidelines 4-5
Fire Control 4-7
Rules of Engagement 4-8
Training and Exercises 4-9
Chapter 5 COMMUNICATIONS 5-1
Overview 5-1
Communications Requirements 5-1
Ground-based Midcourse Defense Networks 5-1
External Sensors 5-3
Responsibilities 5-4
United States Strategic Command 5-4
Joint Functional Component Command-Integrated Missile Defense 5-4
Chapter 6 SECURITY OPERATIONS 6-1
Protection Operations 6-1
Ground-based Midcourse Defense Security 6-1
Security and Defense 6-2
Fort Greely Security 6-6
General Threats to Ground-based Midcourse Defense Resources 6-9
Chapter 7 SUSTAINMENT 7-1
Overview 7-1
Ground-based Midcourse Defense Site Characteristics 7-1
Contractor Logistics Support 7-4
Army Sustainment for Ground-based Midcourse Defense 7-6
SOURCE NOTES ..... Source Notes-1
GLOSSARY Glossary-1
REFERENCES References-1
INDEX Index-1

Figures

Figure 1-1. Ballistic missile phases and ranges 1-2
Figure 2-1. Organization of crew positions 2-2
Figure 2-2. Orbital boost vehicle 2-5
Figure 2-3. Exo-atmospheric kill vehicle 2-6
Figure 2-4. Defense Satellite Program and Space-Based Infrared System satellites 2-7
Figure 2-5. AN/TPY-2 (FBM) with essential support equipment 2-8
Figure 2-6. COBRA Dane radar at Shemya, Alaska 2-9
Figure 2-7. Upgraded early warning radar at Royal Air Force Station Fylingdales 2-10
Figure 2-8. Sea-based x-band radar 2-11
Figure 2-9. Aegis ballistic missile defense destroyer (DDG-70, USS Hopper) 2-12
Figure 3-1. Ground-based Midcourse Defense command relationships 3-3
Figure 3-2. Command relationships 3-5
Figure 3-3. Organizational structure 3-6
Figure 4-1. Example engagement sequence 4-3

Tables

Table 4-1. Example GMD engagement sequence 4-4

This page intentionally left blank.

Preface

Army Techniques Publication (ATP) 3-27.3, *Ground-based Midcourse Defense Operations* provides an overview of Army GMD operations and provides doctrinal principles and procedures outlining how to plan, integrate, and execute GMD operations. ATP 3-27.3 is consistent and compatible with joint and Army doctrine. ATP 3-27.3 links Field Manual (FM) 3-27, *Army Global Ballistic Missile Defense (GBMD) Operations* doctrine at the tactical and operational level to Joint Publication (JP) 3-01, Countering Air and Missile Threats, and at the operational and strategic level to JP 3-27, *Homeland Defense*, as well as United States Strategic Command (USSTRATCOM) Global Ballistic Missile Defense Concept of Operations.

The principal audience for ATP 3-27.3 are all members of the Army Profession. Commanders and staffs of Army headquarters serving as joint task force and multinational headquarters should also refer to applicable joint or multinational doctrine concerning the range of military operations and joint or multinational forces. Other Services and joint organizations may use this publication to gain insight to Army GMD operations. Trainers and educators throughout the Army will also use this publication.

Commanders, staffs, and subordinates ensure their decisions and actions comply with applicable United States, international, and, in some cases, host nation laws and regulations. Commanders at all levels ensure their Soldiers operate in accordance with the law of war, rules of engagement (ROE) and moral and ethical principles inherent in the Army Profession. (See FM 6-27)

ATP 3-27.3 uses joint terms where applicable. Selected joint and Army terms and definitions appear in both the glossary and the text. Defined terms are identified in the text. Terms for which ATP 3-27.3 is the proponent publication (the authority) are marked with an asterisk (*) in the glossary and are boldfaced in the text. For other definitions shown in the text, the term is italicized and the number of the proponent publication follows the definition.

ATP 3-27.3 applies to the Active Army, Army National Guard (ARNG), and United States Army Reserve unless otherwise stated.

The proponent of ATP 3-27.3 is the United States Army Space and Missile Defense Command (USASMDC). The preparing agency is the Unite States Army Space and Missile Defense Center of Excellence. Send comments and recommendations on a Department of the Army Form 2028 (*Recommended Changes to Publications and Blank Forms*) to Director, Army Space and Missile Defense School, Headquarters USASMDC ATTN: SMDC-CE-TI (ATP 3-27.3), 350 Vandenberg Street, Colorado Springs, Colorado 80914, by e- mail to usarmy.peterson.smdc.list.smdc-doctrine@mail.mil, or submit an electronic Department of the Army Form 2028.

This page intentionally left blank.

Introduction

All warfare challenges the moral beliefs and ethical conduct of Army professionals. An enemy may not respect international conventions and may commit atrocities with the aim of provoking retaliation in kind. Any loss of discipline on the part of our Soldiers has the high potential to be exploited in propaganda and magnified through the media. The ethical challenge rests heavily on small-unit leaders who maintain discipline and ensure the conduct of Soldiers remains within ethical and moral boundaries reflected in our Army Ethic. Refer to Army Doctrine Publication (ADP) 1 for information on the Army ethic and Army values.

ATP 3-27.3, *Ground-based Midcourse Defense Operations* is a proponent-level publication. It is the principle publication for describing GMD operations and the Army's GMD mission in defense of the United States homeland, friends, and allies from ballistic missile attack. All aspects of this ATP are consistent with the FM 3- 27, *Army Global Ballistic Missile Defense Operations*. This ATP also establishes the doctrinal framework for GMD Operations in the joint community.

The GMD program provides defense against ballistic missile threats. It consists of specific defensive measures designed to destroy, nullify, or reduce the effectiveness of enemy ballistic missile attacks.

This ATP provides doctrinal guidance on GMD system operations to the Army, the 100th Missile Defense Brigade (100th MD BDE (GMD)) and 49th Missile Defense Battalion (49th MD BN (GMD)) as well as Army Navy/Transportable Radar Surveillance (AN/TPY)-2 Forward Based Mode (FBM) radar support to GMD operations. Operational guidance for GMD is provided by United States Northern Command (USNORTHCOM). Operational guidance for AN/TYP-2 operations is provided by USNORTHCOM and United States Indo-Pacific Command for the Homeland mission.

GMD is an element of the Ballistic Missile Defense System (BMDS) and is the only system for strategic missile defense of the United States homeland. GMD currently protects against the threat of limited intercontinental ballistic missile (ICBM) and intermediate-range ballistic missile (IRBM) attacks. GMD relies on ground-based interceptors (GBIs) based at Fort Greely, Alaska and Vandenberg Air Force Base, California. This fundamental framework guides the Army's participation in GMD system operations. ATP 3-27.3 contains seven chapters:

Chapter 1 provides an overview of ballistic missile defense, describes the GMD mission, and discusses the contributing organizations within the community.

Chapter 2 identifies the major components of the GMD system as well as the contributing sensors and supporting elements.

Chapter 3 identifies the command and control as well as relationships and responsibilities for the organizations involved in countering the global ballistic missile threat.

Chapter 4 discusses GMD fire control operations and associated organizations.

Chapter 5 identifies the communications infrastructure and networks used to make ground midcourse defense a reliable, near real-time reactive system.

Chapter 6 discusses security and protection operations for GMD sites and facilities as well as potential threats which may impact the GMD system.

Chapter 7 discusses site characteristics for sustainment operations as provided by the contract logistic system and the Missile Defense Agency (MDA).

Summary of Changes

As a spiral development program, the Ground-based Midcourse Defense program is constantly evolving. This version of ATP 3-27.3 has been updated to reflect organizational name changes as well as organizational structures, and paragraphs have been added to outline system updates, and to expand upon security issues. A summary of changes is below:

- Updated organizational titles.
- Updated the organizational paragraphs after reorganization.
- Added paragraphs on the Training and Doctrine Command Capability Manager for Strategic Missile Defense, 1st Space Brigade, and the United States Space Command
- Removed reference to the Command Launch Equipment and added the Launch Management System.
- Added paragraphs on Cyber Security, operational contract support, and the logistics civil augmentation program

Chapter 1

Ground-based Midcourse Defense Overview

As the Army's keystone publication for GMD, this publication provides the fundamentals for conducting GMD missile defense operations, describes the Army's role in conducting GMD operations in the joint environment and explains how GMD's tactical operations are linked to strategic operations. This chapter addresses Ballistic Missile Defense concepts, doctrine, the GMD mission, current concepts, and future capabilities.

"The new strategic challenges of the 21st Century require us to think differently, but they also require us to act. The deployment of effective missile defenses is an essential element of the United States' broader efforts to transform our defense and deterrence policies and capabilities to meet the new threats we face. Defending the American people against these new threats is my highest priority as Commander in Chief, and the highest priority of my administration."

President George W. Bush
National Security Presidential Directive 23

SECTION I – GLOBAL BALLISTIC MISSILE DEFENSE OVERVIEW

ARMY GLOBAL BALLISTIC MISSILE DEFENSE MISSION

1-1. The Army is organized to accomplish the ballistic missile defense mission to train, provide for, and equip ground ballistic missile defense forces of all combatant commands. The Army's ballistic missile defense mission is to defend the United States homeland, allies, and forward based forces against all range of missiles in all geographic combatant commander areas of responsibility (AOR), which includes IRBMs with a range between 3,000-5,500 kilometers and ICBMs with a range greater than 5,500 kilometers. Army specific responsibilities are to detect, deter, defend against, and defeat enemy ballistic missile threats (see JP 3-27 and JP 3-01).

1-2. As the lead Service for land-based missile defense, the Army operates elements of the BMDS by planning, coordinating, and executing GBMD operations and integrating GMD with other elements of the BMDS.

1-3. The USASMDC is the Army's proponent for GBMD and provides planning, integration, control and coordination of Army forces, and capabilities in support of USSTRATCOM missions. The GMD system is the only operational system designed to defeat both IRBMs and ICBMs, but is limited to countering a small number of these strategic ballistic missile threats.

1-4. The BMDS is a multi-service, integrated, global system of systems comprised of sensors, weapon systems, command, and information systems. The BMDS provides planning and battle management software and hardware, which employs layered defenses to intercept ballistic missiles during their boost, midcourse, and terminal flight phases. Ballistic missile defense activities do not include defense against cruise or tactical air-to-surface missiles even though some systems are capable of defending against multiple types of threats.

1-5. BMDS capabilities are detection, deterrence, defense against, and the defeat of enemy ballistic missile threats. The goal of the ballistic missile defense is to build an integrated layered BMDS to defeat threat ballistic missiles in all phases of flight. The intent is to be able to engage a ballistic target with multiple weapons systems throughout its entire flight trajectory. For over a half century, space capabilities have enhanced the effectiveness of joint forces during times of peace and times of war, reinforcing the significance of space capabilities when integrated across the range of military operations. Mission planning requires

consideration of space operations across all domains, activities, and processes of an organization to ensure capabilities are available, integrated, and desired effects are delivered.

BALLISTIC MISSILE DEFENSE SYSTEM

1-6. The BMDS consists of a multitude of assets comprising an overall, layered defense. Each asset has unique capabilities and limitations which drives the necessity of a layered defense.

1-7. A ballistic missile does not rely on aerodynamic surfaces to produce lift and consequently follows a ballistic trajectory over most of its flight path. A ballistic trajectory is the path followed after the motor burns out and the remaining parts, such as the body and reentry vehicle (RV) are acted on only by gravity, friction with the air, and winds. A ballistic missile has a prescribed course which generally cannot be altered after the missile has burned its fuel. However, an RV may maneuver independently of the missile or have some form of terminal guidance and control. An RV is the payload of a missile designed to reenter the Earth's atmosphere in the terminal portion of its trajectory and is expected to carry some type of weapons of mass destruction.

1-8. GMD is one part of the layered defenses which use complementary sensors, interceptors, and fire control operations to engage ballistic missile threats in the midcourse phase of flight. The complementary sensors provide data to support multiple engagement opportunities against ballistic missile threats in all phases of flight. Ballistic missile flight is divided into three phases: boost, midcourse, and terminal. Each phase plays an important role in the design of a robust system intended to defend against a ballistic missile attack. Figure 1-1 depicts the ballistic missile flight phases and ranges.

- The boost phase is the segment of flight lasting from launch through the completion of propulsion fuel burn. It is relatively short, usually lasting less than 300 seconds and burning out at an altitude of less than 300 kilometers.
- The midcourse phase begins immediately following booster burnout as the missile and RV continue along their established ballistic trajectory. This phase may last as long as 30 minutes for ICBMs. The GMD system is designed to defend against IRBMs and ICBMs within this phase of flight.
- The terminal phase is the segment of flight where the RV reenters the Earth's atmosphere. This phase usually lasts between 60 and 120 seconds.

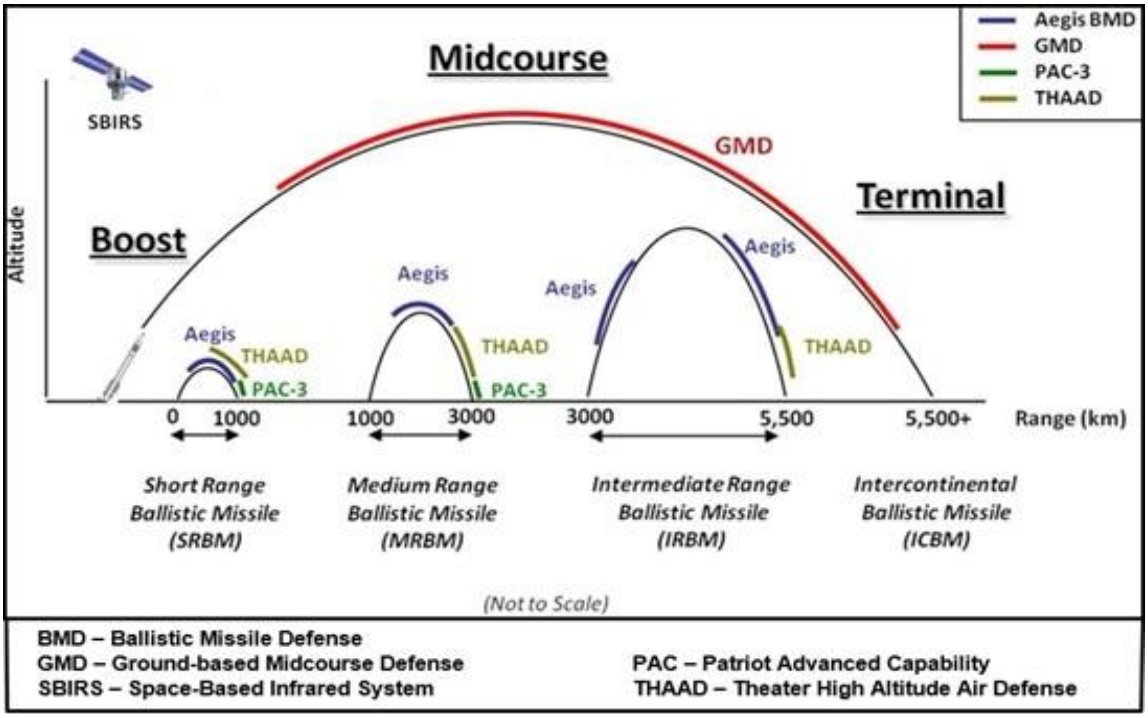

Figure 1-1. Ballistic missile phases and ranges

SECTION II – GROUND-BASED MIDCOURSE DEFENSE OVERVIEW

1-9. Operated by the Army, GMD is the system of ballistic missile defense for homeland defense. The GMD element of the BMDS engages both ICBM and IRBM threats in the midcourse phase of flight using data from a suite of BMDS and external sensors. GMD is contributing to the development of advanced BMDS capabilities with increased data sharing across the system to more effectively manage BMDS assets and prepare the BMDS to engage ballistic missile threats. The technological capability of the system, the mission, and the area to which forces are committed are guiding GMD employment plans and operations as BMDS capabilities evolve in an incremental development process.

MISSION

1-10. The GMD mission is to defend the United States and designated areas against both IRBM and ICBM attacks in the midcourse phase of flight as part of the BMDS and to conduct concurrent operational and test activities. Tasks include:

- Build, test, and verify the defensive operations capabilities;
- Execute concurrent testing and defensive operations;
- Continue development to incrementally improve capability; and
- Provide trained and certified crews, installation support, and site security.

DESCRIPTION

1-11. GMD is the first operational, hit-to-kill and only operationally deployed missile defense program to defend the homeland against long-range ballistic missile attacks. The system provides early detection and tracking during the boost phase, midcourse target classification and discrimination, precision intercept and destruction of inbound IRBMs or ICBMs through the force of kinetic kill technology. GMD uses multiple sensors, communications systems, fire control capabilities, and GBIs which are capable of detecting, tracking, and destroying IRBMs and ICBMs during the midcourse phase of flight. The GMD system is comprised of the ground systems, GBI, and sensors.

1-12. The ground system is made up of the GMD fire control, in-flight interceptor communication system (IFICS), launch support system, and GMD communications network. The GMD fire control orchestrates the battle and is operated by Soldiers who ensure the USNORTHCOM commander’s intent is met for each threat. The GMD communications network links the components of the system together to provide seamless information exchange via fiber optic cables and satellites. The GMD fire control system communicates with an exo-atmospheric kill vehicle (EKV) during flight via an IFICS data terminal. The launch support system communicates with the GBI on the ground and passes information between the GMD fire control and the GBIs.

1-13. The GBI is comprised of the Orbital boost vehicle in a standardized three-stage booster configuration. The Orbital boost vehicle carries the booster avionics module and the EKV into its trajectory. The EKV is a sensor-propulsion package designed to destroy the incoming RV using kinetic energy through collision with the target. The hit-to-kill method uses proven technology verified in multiple flight tests using operationally configured GBIs.

1-14. Space, sea, and ground-based sensors support the GMD by providing data the system relies upon to calculate firing solutions. These sensors provide target search, acquisition, track, classification, discrimination, and other system data to the GMD system to support successful EKV engagement against threat objects. This information provides the EKV with the ability to locate, discriminate, and destroy the incoming RV.

1-15. The MDA continuously performs testing and development in order to improve the system's ability to counter the capabilities of the evolving threat. As technology advances, they performs incremental capability development concurrently with operations in order to improve the system's capabilities without interrupting its operational capabilities. These incremental improvements could include updating or adding sensor

resources, improving the GBI and EKV technologies, upgrading GMD fire control software, and improving the communications and control capabilities within the GMD architecture.

OPERATIONAL ENVIRONMENT

1-16. An operational environment is a composite of the conditions, circumstances, and influences that affect the employment of capabilities and bear on the decisions of the commander (JP 3-0). An operational environment includes physical areas (air, land, maritime, and space domains) and the information environment, which includes cyberspace domain. An operational environment includes isolated conditions of interacting variables existing within a specific area of operations, but also interconnected influences from global or regional perspectives, such as political, cultural, and economic influences impacting conditions and operations.

Note. An operational environment in which a unit conducts operations should not be confused with training environments created by the commander for local training.

1-17. Analysis of the broad aspects of an operational environment in terms of the operational variables provides relevant information senior commanders use to understand, visualize, and describe the operational environment. The operational variables are political, military, economic, social, information, infrastructure, physical environment, and time. Upon receipt of a warning order or mission, Army commanders filter relevant information and narrow their focus to six mission variables. The mission variables are mission, enemy, terrain and weather, troops and support available, time available, and civil considerations. These variables are used during intelligence analysis and to facilitate situational awareness and understanding (see ADP 3-0).

1-18. Due to the distributed nature of the GMD architecture, GMD encompasses all physical and information areas of the operational environment. See chapter 2 for those assets which occupy the physical domain and chapter 5 for the communications architecture which occupies the information environment.

RISK MANAGEMENT

1-19. Commanders use several integrating processes and continuing activities while conducting ballistic missile defense operations. The military decision-making process and risk management should be applied during planning. Overall operations must be synchronized and fully integrated with each other.

1-20. Risk management is the Army's process for identifying hazards and controlling risks across the range of military operations, missions, functions, and activities. It is used to mitigate risks associated with all hazards which have the potential to injure or kill personnel, damage or destroy equipment, or otherwise impact mission effectiveness. Army leaders take prudent risks and make risk decisions based on informed judgment and intuition. Lack of inclusion of information operations and space-related information during mission assessment may lead to an inaccurate risk assessment for the mission. Risk management is a function of the probability of an event occurring and the severity of the event expressed in terms of the degree to which the incident affects combat power or mission capability.

1-21. Risk management is a five-step process. It serves as an integrating process for the Protection warfighting function in Army operations. The process subjectively quantifies probability and severity using the Army risk assessment matrix, leading to a determination of the risk level. Risk levels help show relative significance and serve to alert and inform leaders as they make decisions regarding course of action selection and resource allocation. Risk management also helps leaders decide where and when to apply protection assets and information. A few missile defense-related risk management items to consider during every mission planning and execution risk assessment include, but are not limited to, information protection, personnel safety, safety zones, security, and in the case of GMD, the risk of not acting on threats. Refer to ATP 5-19 for more information on the risk management process.

1-22. BMDS radio frequency emissions make emplacement considerations critical. The planners must ensure no other equipment is placed inside the keep out zone. The keep out zone varies for each system based on specific power output, but may extend out from a radar face in excess of 10 kilometers and sweep more than 70 degrees on each side from the system bore sight. Site personnel shall conduct routine functional tests

of all warning devices and interlock systems to ensure proper function. An audible signal shall be automatically activated by the radar equipment to alert personnel the system is about to radiate. Site personnel must receive initial and routine briefings on system hazards and the radiation protection program. Before radiating or going to remote operation, site personnel must ensure all crew members have vacated the personnel keep out zone directly in front of the system.

Note: Dangerous radio frequency power levels exist on and near antennas and phased-array radars during operations. Radio frequency electromagnetic radiation may cause serious burns and internal injury. All personnel must observe radio frequency danger indications and stay outside designated keep out zones.

DEFINITIONS

1-23. Ballistic missile - Any missile which does not rely upon aerodynamic surfaces to produce lift and consequently follows a ballistic trajectory when thrust is terminated (JP 3-01).

1-24. BMDS – An evolving, [Joint] integrated, and interoperable system comprising multiple elements and components that will provide opportunities to intercept ballistic missiles in all phases of flight (boost, midcourse, and terminal) against all ranges of threats according to the Department of Defense directive (DODD) 5134.09, 17 September 2009. The BMDS consists of a layered system of systems comprised of sensors, weapon systems, planning and battle management software and hardware.

1-25. GBMD – Defense against ballistic missile threats that cross one or more geographical combatant command boundaries and requires synchronization among the affected combatant commands (JP 3-01).

1-26. GMD – A surface to air BMDS for exo-atmospheric midcourse phase interception of long- range ballistic missiles using the ground-based interceptors (JP 3-01). GMD consists of multi-service and multi-agency assets utilized for strategic missile defense of the United States homeland. The Army is the lead Service for the GMD system which is an element of the BMDS. It functions under the USSTRATCOM GBMD concept for defending the United States, its forces, and its allies from ballistic

GROUND-BASED MIDCOURSE DEFENSE CONTRIBUTING ORGANIZATIONS

1-27. This section discusses GMD contributing organizations. It covers various commands, organizations, and agencies which contribute to the GMD mission.

UNITED STATES STRATEGIC COMMAND

1-28. Located at Offutt Air Force base near Omaha, Nebraska, USSTRATCOM is one of ten unified commands in the Department of Defense. Its mission is to conduct global operations in coordination with other combatant commands, Services, and appropriate United States government agencies to deter and detect strategic attacks against the United States and its allies, and is prepared to defend the nation, as directed. USSTRATCOM integrates and coordinates the necessary command and control capability to provide support with the most accurate and timely information for the President, the Secretary of Defense, other national leadership and other combatant commanders.

1-29. Commander, USSTRATCOM is the supported commander for GBMD planning and coordinating ballistic missile defense operations support. Commander, USSTRATCOM is the supporting commander to USNORTHCOM for the execution of the GMD mission, but has combatant command authority for the 100th MD BDE (GMD) and the 49th MD BN (GMD).

JOINT FUNCTIONAL COMPONENT COMMAND FOR INTEGRATED MISSILE DEFENSE

1-30. The Joint Functional Component Command for Integrated Missile Defense (JFCC-IMD) began operations in January 2005. The Command includes Army, Navy, Marine Corps, and Air Force personnel, as well as United States government civilians and contractor personnel. JFCC-IMD headquarters is located in the Missile Defense Integration and Operations Center at Schriever Air Force base, Colorado. JFCC-IMDs

location allows them to leverage strong partnership with the material developer to execute all of their assigned responsibilities.

1-31. JFCC-IMD synchronizes missile defense planning, conducts ballistic missile defense operations support, and advocates for missile defense capabilities in support of USSTRATCOM, other combatant commands, the Services, and appropriate United States government agencies, to deter adversaries, assure allies, and defend the United States, deployed forces, allies and partners against missile attacks.

JOINT FORCE SPACE COMPONENT COMMAND

1-32. The Joint Force Space Component Command (JFSCC) is a component of USSTRATCOM and is responsible for executing continuous, integrated space operations to deliver theater and global effects in support of national and combatant commander objectives. The JFSCC coordinates space operational- level planning, integration, and coordination to ensure unity of effort in support of military and national security operations, and support to civil authorities.

DEFENSE INTELLIGENCE AGENCY

1-33. The Defense Intelligence Agency provides military intelligence to warfighters, defense policymakers and force planners in the Department of Defense and the Intelligence Community, in support of U.S. military planning and operations and weapon systems acquisition. The agency plans, manages, and executes intelligence operations during peacetime, crisis, and war.

UNITED STATES NORTHERN COMMAND

1-34. USNORTHCOM deters ballistic missile attacks on the United States, its territories, possessions, and bases within its AOR and other areas as directed. Should deterrence fail, and as directed by the Secretary of Defense, commander, USNORTHCOM will employ available ballistic missile defense forces to defeat ballistic missile attacks.

1-35. The commander, USNORTHCOM is the supported commander for homeland defense. USNORTHCOM has operational control (OPCON) for execution of the ballistic missile defense for the homeland defense mission. Army Forces Command provides missile defense forces under command of USSTRATCOM to execute ballistic missile defense operations for the defense of North America. These forces are OPCON to USNORTHCOM.

NORTH AMERICAN AEROSPACE DEFENSE COMMAND (NORAD)

1-36. NORAD provides aerospace warning for North America which consists of the detection, validation, and warning of an attack against North America, whether by aircraft, missiles, or space vehicles. NORAD has three missions: aerospace warning, aerospace control, and maritime warning. NORAD's core responsibilities include:

- Deter, detect, and defend against aerospace threats to North America; and
- Provide timely and accurate, integrated tactical warning and attack assessment to North America

UNITED STATES INDO-PACIFIC COMMAND

1-37. Commander, United States Indo-Pacific Command is supporting commander to Commander, USNORTHCOM for missile defense of the contiguous 48 states, Alaska, and Hawaii. Commander, United States Indo-Pacific Command is supporting commander to commander, USSTRATCOM for planning, integrating, and coordinating global missile defense operations and support to missile.

UNITED STATES SPACE COMMAND

1-38. The United States Space Command mission is to deter aggression and conflict, defend U.S. and allied freedom of action, deliver space combat power for the Joint/Combined force, and develop joint warfighters to advance U.S. and allied interests in, from, and through the space domain.

COMBINED FORCE SPACE COMPONENT COMMAND

1-39. The Combined Force Space Component Command will plan and execute space operations through four distinct and geographically dispersed operations centers, including: the Combined Space Operations Center at Vandenberg AFB, California; Missile Warning Center at Cheyenne Mountain Air Force Station, Colorado; Joint Overhead Persistent Infrared Center at Buckley AFB, Colorado; and Joint Navigation Warfare Center at Kirtland AFB, New Mexico. Additionally, the Combined Force Space Component Command will execute tactical control over globally dispersed Air Force, Army, and Navy space units that command satellites in every orbital regime.

UNITED STATES ARMY SPACE AND MISSILE DEFENSE COMMAND

1-40. USASMDC is an operational level Army force designated by the Secretary of the Army and serves as the Army Service component command to USSTRATCOM which is the integrator for GBMD. USASMDC serves as Army's integrator for GBMD based on Army Regulation (AR) 10-87 and General Order 37. USASMDC provides planning, integration, control, and coordination of Army forces and capabilities in support of USSTRATCOM missions.

UNITED STATES ARMY SPACE AND MISSILE DEFENSE SCHOOL

1-41. As the Army's proponent for global missile defense, USASMDC is responsible for providing mission training for GMD personnel as well as AN/TPY-2 (FBM) sensor managers and radar operator/maintainers. The U.S. Army Space and Missile Defense School supports USASMDC by developing and conducting an array of courses including the GMD Qualification Course, AN/TPY-2 (FBM) Sensor Manager Qualification Course, and GMD System Trainer Course. These courses are accredited Army courses and are scheduled via the Army Training Requirements and Resource System.

TRAINING AND DOCTRINE COMMAND CAPABILITY MANAGER FOR STRATEGIC MISSILE DEFENSE

1-42. The Training and Doctrine Command Capability Manager for Strategic Missile Defense (SMD) serves as the capability integrator for current and future SMD capabilities with a focus on Army equities of the weapons, sensors, and battle management systems constituting the SMD architecture. The SMD architecture currently includes, but is not limited to the GMD program, AN/TPY-2 (FBM) Radars and the Command and Control, Battle Management, and Communications (C2BMC) system.

1-43. As the Army's centralized capability developments integrator for SMD operations, the Training and Doctrine Command Capability Manager for SMD is the user's advocate for all doctrine, organization, training, materiel, leadership and education, personnel, facilities, and policy (DOTMLPF-P) solutions for SMD. The Training and Doctrine Command Capability Manager for SMD coordinates and integrates DOTMLPF-P solutions with other force modernization proponents, materiel developers (e.g. Missile Defense Agency), and provides input and reviews capability requirements documents for assigned SMD capabilities. These capability areas require long-term management due to their comprehensive and enduring nature. The Training and Doctrine Command Capability Manager for SMD monitors all DOTMLPF-P related activities during a system's development to maintain a path towards successful system fielding.

1ST SPACE BRIGADE

1-44. Assigned to the 1st Space Brigade, the personnel within the AN/TPY-2 (FBM) batteries operate and sustain the radars and perform theater, medium, and long-range search and target acquisition in support of GBMD missions.

100TH MISSILE DEFENSE BRIGADE (GMD)

1-45. The mission of the 100th MD BDE (GMD) is, on order, to destroy ICBMs in the midcourse phase of flight to defend the United States and additional designated areas. The 100th MD BDE (GMD) organizes and trains soldiers to operate the GMD fire control system. They also provide planning and coordination functions

for GMD test and exercise activities. The operational elements of the 100th MD BDE (GMD) are OPCON to USNORTHCOM and execute the homeland mission as directed by commander, USNORTHCOM.

1-46. The 100th MD BDE (GMD) Commander serves dual-status in both a Title 10 and Title 32 United States Code capacity to effectively command multi-component Soldiers. The 100th MD BDE (GMD) is comprised of both Active Army and ARNG Active Guard Reserve (AGR) Soldiers who operate the missile defense element (MDE) at Schriever Air Force base, one of the two GMD fire control nodes. The MDE operates continuously, utilizing a five-crew rotation schedule with five unique crew positions. The 100th MD BDE (GMD) also exercises OPCON over the 49th MD BN (GMD).

1-47. The 49th MD BN (GMD) provides AGR Soldiers to operate the fire direction center (FDC) at Fort Greely, Alaska, the second of the two GMD fire control nodes. The mission of the 49th MD BN (GMD) is two-fold; to operate and secure the GMD system at Fort Greely, and on order, to destroy ICBMs in the midcourse phase of flight to defend the United States and defended areas. The 49th MD BN (GMD) is comprised of only AGR Soldiers. The FDC operates continuously, utilizing five unique crew positions, similar to the MDE, but with additional responsibilities, such as monitoring of the ground safety device.

1-48. The mission of the 100th MD BDE (GMD) Detachment 1 is to provide continuous monitoring, safety and enabling of the ground safety device at Vandenberg Air Force Base. They interface with the MDA and Boeing to ensure the GBIs for which they are responsible, are available and mission capable. Liaise with the 100th MD BDE leadership to provide the health and status of GMD assets located at Vandenberg Air Force Base and support the 49th MD BN and the 100th MD BDE missile defense crews during crisis and combat operations.

1-49. The Fort Drum Security Detachment is in place to provide security for the GMD resources located at Fort Drum, New York. This detachment consists primarily of Department of the Army civilians who are supervised by military personnel.

UNITED STATES ARMY AIR AND MISSILE DEFENSE COMMANDS

1-50. The United States Army Air and Missile Defense Commands (AAMDC) perform regional air and missile defense planning, integration, coordination, and execution functions for the Army force commander and joint force land component commander. The AAMDCs directly coordinate global and strategic missile issues with USSTRATCOM, JFCC-IMD, and USASMDC GBMD planners. From the missile defense perspective, the AAMDCs are a lateral force with which direct coordination is authorized.

1-51. The AAMDCs support GMD operations by controlling the AN/TPY-2 (FBM) radars to provide early warning of strategic threats against the homeland and regional missile defense for designated assets and defense of AOR. In theater, the AAMDCs also conducts joint and combined strategic air and missile defense to support designated operations plans, contingency operations, and homeland defense.

MISSILE DEFENSE AGENCY

1-52. Deployed BMDS capabilities are for potential operational use globally. The MDA is continuously developing and deploying missile defense systems for the Department of Defense (DOD) capable of protecting the United States homeland, our deployed forces, friends, and allies. As the lead agency for BMDS development, their charter is to provide centralized management for the development and integration of sensors, interceptors, command, and battle management of the systems into the GBMD framework. Specifically, they are directed per Executive-level and DOD-level guidance to:

- Develop and deploy, as directed, a layered BMDS;
- Enable the fielding of elements of the BMDS as soon as practicable; and
- Provide capability in block increments, improving the effectiveness of fielded capability by inserting new technologies as they become available.

Chapter 2

Components

This chapter provides descriptions of the ground system, GBI and external contributing elements which support the GMD mission. Many components provide battle management, command, control, communications, and operate in conjunction with, or in direct support of, other external supporting systems. This chapter also covers sensors used to provide GMD systems with target search, early threat detection, acquisition, track, classification, hit assessment, and GBI control.

SECTION I – GROUND-BASED MIDCOURSE DEFENSE GROUND SYSTEM

2-1. The GMD ground system is the integrating and controlling component of the GMD element. The ground system components consist of the equipment, communications, operations, procedures and personnel essential for planning, directing and controlling operations of assigned assets to accomplish the GMD mission. Ground systems include:

- GMD fire control nodes;
- Launch support system;
- Ground safety device;
- IFICS; and
- GMD communications network (detailed in chapter 5).

GROUND-BASED MIDCOURSE DEFENSE FIRE CONTROL

2-2. The GMD fire control system is the core of the GMD architecture. It is a suite of hardware, software, and specially trained personnel integrating GMD and supporting elements to manage all phases of engagement. This system provides engagement operations with predictive planning, potential for automated execution of certain functions, and serves as the human-in-control interface. Based on input from ballistic missile defense sensors, the system assesses flight paths of the incoming threats, determines impact locations, and prepares defend task plans for the GMD resources. The fusing of this information allows the EKV to locate, discriminate, and destroy its intended target. The functions and capabilities include mission command, battle management, decision support, communications, training, testing, and intelligence.

2-3. The interactive capability allows control and direction of the battle in near real-time. This includes turning the engagement execution on and off, modifying engagement parameters, and managing exceptions and anomalies. The operators bring external information and intelligence, such as the concern of potential follow-on attacks and the nature of the threat, to the engagement. The intelligence drives the modification of pre-determined defense strategies (DS) and execution plans (XP). While the DS and XP are separate applications, neither is used in battle by itself; they are symbiotic in nature and always referred to as DS/XP functions. The interactive capability and symbiotic function ensure operators maintain full control of the fire control system.

2-4. The GMD fire control engagement planner is the automated software program. It consolidates and synthesizes all the sensor data, builds and sends sensor task plans to cue sensors to begin tracking the objects, develops the weapons task plan for the GBI, provides guidance to the GBI and EKV, and provides system status information to the operators. The engagement planner begins building a firing solution as soon as the system detects a ballistic missile and identifies it as threat to the defended areas. As sensors continue to track and analyze the threat, the refined track data is transmitted to the EKV to aid its intercept of the target. GMD operators monitor all of the threat's characteristics to determine the best course of action to meet the commander's intent.

2-5. Both space and terrestrial-based communications systems provide communications paths through the GMD fire control system through an IFICS data terminal, and on to an EKV. The communications capability provides connectivity among supporting sensors, ground-based elements, and GMD fire control capabilities located in various operations and control centers. Reliable, redundant communications is necessary among the MDE, FDC, and alternate facilities to ensure all GMD systems components are operating effectively.

2-6. The GMD fire control system has an embedded test and exercise capability which allows operators to conduct training and exercises concurrent with day to day operations. This capability allows the GMD operators to conduct distributed or stand-alone training and test operations in order to maintain proficiency, evaluate hardware, software and tactics, techniques and procedures. The fire control system also has an embedded testing capability allowing the injection of periodic system tests into the operational system without disrupting operational readiness.

2-7. The GMD fire control system also has an embedded external system interface providing interface management and message transfer between the GMD fire control system and external elements with a variety of interface protocols.

FIRE CONTROL NODES

2-8. The GMD system consists of two operational fire control nodes, the MDE and FDC. They are organized similarly and conduct the operational level execution of the GMD mission. Each node is staffed continuously with five primary crewmembers who provide direction to the fire control system based upon coordination with the NORAD-USNORTHCOM Command Center Director through the missile defense officer (MDO). Figure 2-1 shows the MDE and FDC corresponding crewmember positions and rank of each crewmember.

2-9. While operating the fire control system, crewmembers are under OPCON of the commander, USNORTHCOM. Operating under nominal conditions, with both nodes operational, each node has its own set of responsibilities, however, either node may assume the duties of the other in a failover operation and execute current missile defense operations. Auxiliary GMD fire control work stations exist inside each fire control node to provide workstation redundancy. A few GMD fire control terminals exist at designated operations centers and are configured to provide situational awareness; they do not permit fire control execution.

Missile Defense Element (MDE) Positions				
Director	Deputy Director	Current Operations Officer	Future Operations Officer	Readiness Officer
LTC/O5	MAJ/O4	CPT/O3	SFC/E7	SSG/E6

Fire Direction Center (FDC) Positions				
Director	Deputy Director	Sensors Operator	Weapons Operator	Communications Operator
MAJ/O4	CPT/O3	1LT/O2	SSG/E6	SGT/E5

1LT: Fist Lieutenant LTC: Lieutenant Colonel SFC: Sergeant First Class SSG: Staff Sergeant
CPT: Captain MAJ: Major SGT: Sergeant

Figure 2-1. Organization of crew positions

Missile Defense Element

2-10. The 100th MD BDE (GMD) is responsible for staffing MDE crews. Nominally, the MDE provides operational and tactical recommendations to the combatant commander, synchronizes operations, and directs

the tactical fight through the FDC crews. The MDO relays weapons control direction from commander, USNORTHCOM to the MDE Director who then orders changes to the weapons control status. The MDO cannot accomplish a weapons control order action; it requires two crewmembers at the same node; one to initiate and one to confirm the order to change weapons control status from hold-to-free or free-to-hold. The MDE plans future battles in coordination with the MDO and FDC deputy director, monitors the current battle, provides expertise for system performance and readiness, and provides situational awareness reports through the MDO to commander, USNORTHCOM. As required, the MDE will assess the missile warning and defense common operational picture for potential follow-on launches. It manages day-to-day control of the FDC, readiness conditions, and develops and reports overall GMD system capability.

Fire Direction Center

2-11. The 49th MD BN (GMD) is responsible for staffing FDC crews. The FDC is co-located with the missile fields on Fort Greely, and will fight the current battle based upon direction from the USNORTHCOM command center director and the MDE. The FDC will conduct missile engagements by executing management-by-exception redirection criteria in accordance with the commander's intent and directives.

SILOS

2-12. The GBIs are housed in silos at missile fields on Fort Greely and in launch facilities at Vandenberg Air Force Base. The missile complex facilities support the integration and maintenance of the GBIs. These facilities are comprised of the missile assembly building, mechanical electrical building, interceptor storage facilities, EKV fuel storage, and EKV oxidizer storage facilities.

LAUNCH SUPPORT SYSTEM

2-13. The launch support system controls the operations of the GBIs during ground operations through launch. It maintains the GBIs in a state of readiness to perform their function, generates flight data from the weapons task plan, and sequences Interceptors into a launch posture. In addition, it provides the facilities, services, and transport equipment to support the GBIs and their payload throughout their operational life while also controlling the maintenance activities while a portion of a GBI is in maintenance mode. The launch support system consists of the launch management system (LMS), launch site components, and peculiar support equipment.

LAUNCH MANAGEMENT SYSTEM

2-14. The LMS at Vandenberg Air Force Base, Fort Greely, and at any future missile launch sites are essential components of the GMD system. The LMS provides the vital connectivity between the GMD fire control system and the GBIs prior to launch.

2-15. The LMS component of the launch support system is comprised of the GBI maintenance managers and GBI launch managers. The GBI maintenance managers communicate with the GBI launch managers in order to monitor and control GBIs and supporting silo hardware.

LAUNCH SITE COMPONENTS

2-16. The launch site components consist of the silo, the silo interface vault, and silo closure mechanism. The launch site components are responsible for maintaining and monitoring the internal temperature and humidity levels and supporting all site maintenance activities. The launch site components consist of the components and equipment necessary to provide a sheltered environment for the GBI and the launch station equipment portion of the LMS used to interface with the Interceptor. The launch site components provide control of and monitoring of the health and status of the launch site components environmental control system.

2-17. The silos are structures which house the GBIs. The silos orient the GBIs to a globally fixed position for guidance, navigation and control reference. It provides a plumbed and clocked capability for registering the GBI. It also separates the GBI from the Earth and provides a stable, ready state environment for the planned dormancy periods.

2-18. Each silo interface vault contains the launch station equipment component of the LMS communicate with the interceptor for test, maintenance, and pre-launch. The silo interface vault interface panel contains the electrical umbilical, re-radiation coax cables, and test measurement and diagnostic equipment lines routed to the Interceptor. The launch site components provide the lateral support group in the silo to assist the boost vehicle with lateral stability while in the silo. The launch site components provide conditioned air through an umbilical to support the payload. The launch site components provide retraction mechanism(s) for the air supply umbilical.

2-19. The silo closure mechanism allows for access through the top of the silo for the insertion of the interceptor, maintenance, and or removal of the interceptor from the silo. The capability for rapid opening allows the interceptor to meet the launch timelines it receives from the GMD fire control based upon information obtained from various sensors. In addition, the covered top serves to protect and isolate the interceptor from natural, hostile, and induced environments. If left unprotected, the operational readiness of the interceptor may be affected.

PECULIAR SUPPORT EQUIPMENT

2-20. The peculiar support equipment is a component of the launch support system and consists of support handling equipment, test measurement and diagnostic equipment, and non-tactical equipment. Its function is to provide support and handling equipment for the weapon system and all of these elements are required to safely handle, transport, store or install the payload into the silo.

2-21. The support handling equipment required to transport and emplace GBIs includes tractors, trailers, erectors and ancillary equipment needed to load, transport, transfer, and erect the interceptor. Also included is any specialized support and handling equipment required for installation of the launch ground communications equipment, launch station equipment, and readiness station equipment. This equipment is restricted to specialized equipment not commonly provided by the facilities.

2-22. The test measurement and diagnostic equipment fulfils a requirement to test selected payload components during assembly. Additionally, the specialized test measurement and diagnostic equipment supports developmental tests and operational deployment of the weapon system.

GROUND SAFETY DEVICE

2-23. The ground safety devices are operator controlled switch panels providing a series of electro-mechanical switches allowing the operator to inhibit or enable launch communications between the LMS and the GBIs. The ground safety device provide a vital connectivity between the GMD fire control and the LMS, and provide a safety mechanism via human-in-the-loop to prevent inadvertent launches of GBIs.

IN-FLIGHT INTERCEPTOR COMMUNICATIONS SYSTEM

2-24. The IFICS is a dedicated communication system for GMD consisting of a high- powered communication terminal and antenna capable of communicating with GBIs in flight. IFICS establishes and supports nuclear-survivable data communication links between the IFICS data terminals and the in-flight interceptors or EKVs. The IFICS data terminals provide communications support for the transmission of in-flight target updates from the GMD fire control to the GBI and the reception of the in- flight status reports from the interceptor to the GMD fire control. Since the GBIs travel long distances, the IFICS must be located in diverse sites over a broad area to ensure line-of-sight with the GBIs at all times.

SECTION II – GROUND-BASED INTERCEPTOR

2-25. The GBI is designed to deliver the EKV to a particular point along a RV's flight path allowing it to intercept RVs outside the Earth's atmosphere (exo-atmospheric), destroying them kinetically. The GBI consists of two components, a multi-stage, solid propellant orbital boost vehicle and the payload which consists of the booster avionics module and the EKV. The orbital boost vehicle is a high-powered rocket used to propel the EKV to its intercept basket outside the atmosphere and is housed in an underground launch silo. The range and speed of the booster allows the GBI to defend much of the homeland.

ORBITAL BOOST VEHICLE

2-26. The Orbital boost vehicle consists of a three-stage vehicle designed to propel the payload onto its trajectory of flight. The Orbital boost vehicle is a commercially designed, off the shelf model used in the Pegasus program and is the boost vehicle employed on all operational GBIs. The payload is located on the top of the boost vehicle and has a protective shroud designed to cover the payload during initial flight through the atmosphere. In preparation of independent EKV operations, the shroud is released and falls away from the boost vehicle in the upper atmosphere shortly after the second stage separates and ignites from the first stage. The booster avionics module allows the use of an EKV on a variety of boost vehicles as they become available. The booster avionics module assists in flight control during the boost phase, supports the EKV during boost and separation, and propels the EKV into its trajectory of flight when released from the third stage booster. The orbital boost vehicle with payload is shown in figure 2-2.

2-27. The GBIs reside in underground launch silos which serve as both the housing and alignment for the Orbital boost vehicles. The silos provide protection to the boosters from attacks as well as protection from the external environment. Additionally, the controlled environment inside the silos helps protect critical components from rapid degradation and facilitates routine maintenance.

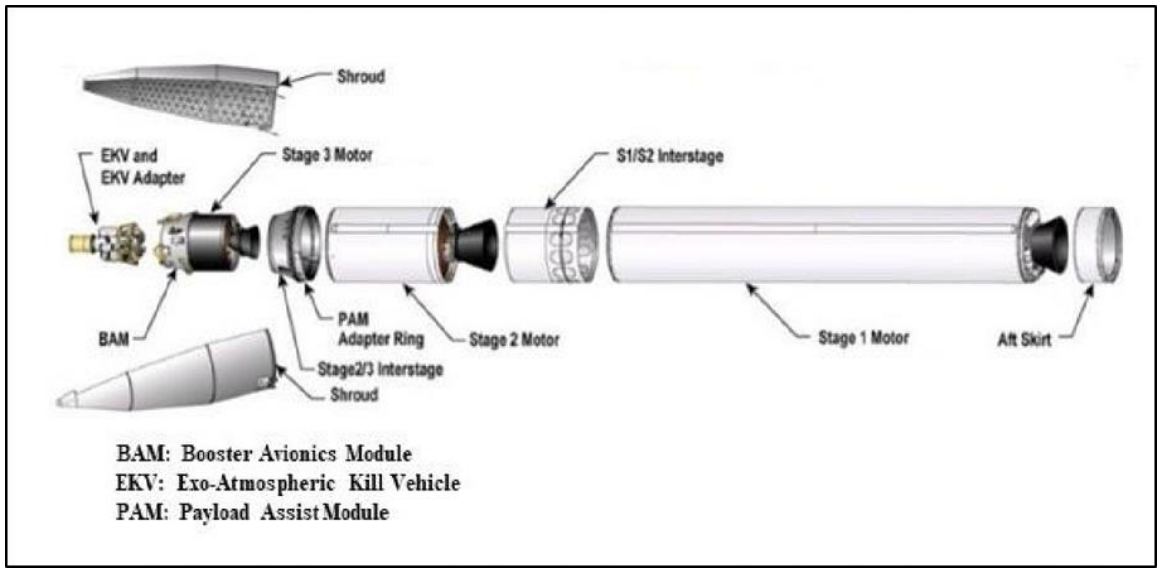

Figure 2-2. Orbital boost vehicle

EXO-ATMOSPHERIC KILL VEHICLE

2-28. The EKV is the kill vehicle of the GBI. The GMD fire control generates and sends a weapons task plan to the GBI. The EKV receives nominal target characterization during the GMD fire control mission data load just prior to its launch and during in-flight updates. Upon being delivered to a point in space by the booster, the EKV's infrared seeker and flight package perform all navigation, guidance, and control activities necessary to engage the target. The EKV autonomously discriminates the threat object through its integrated onboard sensor suite and processing algorithms.

2-29. While the interceptor is in-flight, the EKV receives communications from, and transmits communications to, the IFICS. The initial communications event consists of an in-flight target update which is generated by the GMD fire control and transmitted to the EKV; the EKV responds by sending an in-flight status report message back to the GMD fire control to update its status. During subsequent communication, the GMD fire control generates a second in-flight target update to relay final track data to the EKV. The interceptor uses the data provided by the in-flight target updates to acquire the cluster of potential threat objects and discriminate the potential threat objects from decoys and debris. When it reaches its acquisition range, the EKV autonomously tracks, discriminates objects, engages the threat object, and destroys it kinetically. The EKV is shown in figure 2-3, on page 2-6.

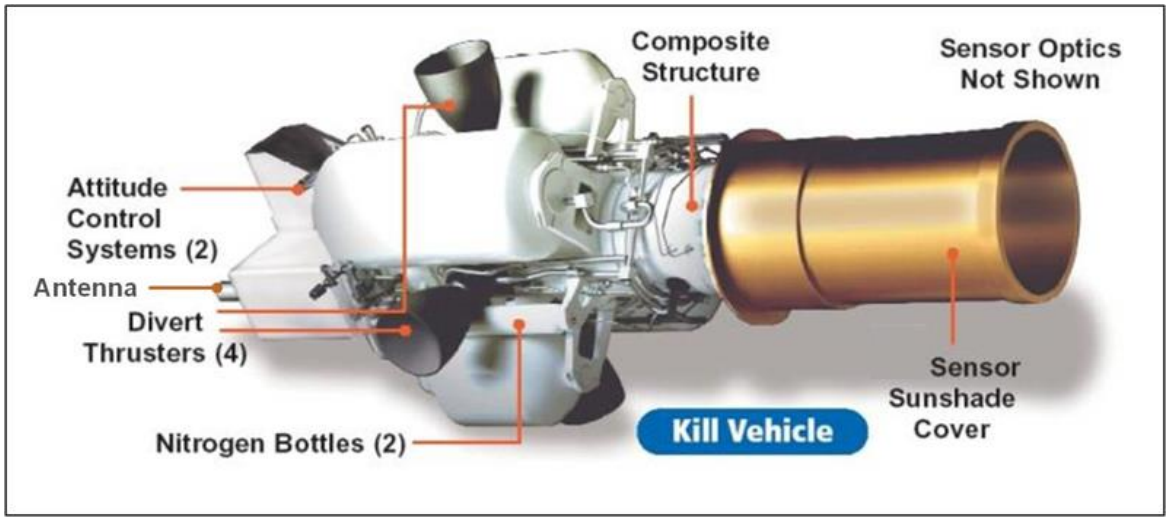

Figure 2-3. Exo-atmospheric kill vehicle

SECTION III – CONTRIBUTING SENSORS AND ELEMENTS

2-30. Ballistic missile defense contributing sensors make up a systems-of-systems consisting of early warning sensors in space, on land, and at sea to provide data to enhance engagement operations. Ballistic missile defense sensors also provide synchronization and integration of capabilities to destroy or disrupt enemy missiles. Early warning sensors are a key element to defense of the United States homeland.

SPACE DOMAIN

2-31. Overhead persistent infrared are those systems originally developed to detect and track foreign intercontinental ballistic missiles. The infrared signature created by the combustion of the missile's fuel provides a highly visible exhaust plume and increases the likelihood of detection by satellite sensors. Overhead persistent infrared satellites use sensors to detect infrared energy (heat) from missile and booster plumes against the Earth's cooler background and are able to track ballistic missiles from launch through booster burnout. Overhead persistent infrared satellites provide early warning of missile launches and usually provide the first indication of a missile launch. Both Defense Satellite Program and space-based infrared system (SBIRS) satellites are overhead persistent infrared systems. Both Defense Satellite Program (DSP) and space-based infrared system (SBIRS) satellites are overhead persistent infrared systems shown in figure 2-4.

Figure 2-4. Defense Satellite Program and Space-Based Infrared System satellites

2-32. The SBIRS constellation is composed of Defense Satellite Program and SBIRS satellites comprising the space segment used to enable the GMD mission. Defense Satellite Program satellites are legacy vehicles in a geosynchronous Earth orbit while the SBIRS satellites—the current lineage of satellites—can reside in both a geosynchronous Earth orbit and a highly elliptical Earth orbit. Since ground-based sensors cannot observe and characterize a target being blocked by the Earth, a space-based system provides early target characterization and tracking information before surface-based sensors detect the targets.

2-33. The SBIRS constellation provides the initial ballistic missile launch detection with continuous global coverage. Information received from the satellites is relayed to the SBIRS mission control station where it is injected into the GMD communications network and Fire Control System. SBIRS is part of the integrated tactical warning and attack assessment system and provides the GMD fire control with a launch location, launch time, and predicted point of impact. SBIRS data provides initial indications of a launch and is used to cue other systems to begin searching specified locations for ballistic missiles.

LAND DOMAIN

2-34. The land-based components are the primary radar sensors used to enable the GMD mission. They consist of AN/TPY-2 (FBM) radars, upgraded early warning radars (UEWR), and the COBRA Dane radar. The AN/TPY-2 (FBM) radars are forward deployed acquisition and tracking radars; the COBRA Dane and UEWRs are fixed sensors used to support long-range acquisition and tracking. These sensor systems provide early target characterization and tracking information, permitting launch of a correctly tailored interceptor package during midcourse intercepts.

AN/TPY-2 FORWARD BASED MODE RADAR OPERATIONS

2-35. The Army Navy/Transportable Radar Surveillance and Control Model 2, or AN/TPY-2, is a transportable X-band, high-resolution, phased-array radar designed specifically for ballistic missile defense. The AN/TPY-2 radar is capable of tracking all classes of ballistic missiles and identifying small objects at long distances. In the forward-based mode, this radar plays a vital role in the BMDS by detecting ballistic missiles early in their flight and providing precise tracking information for use by the GMD fire control system. Use of multiple sensors provides complementary sensor coverage, expands the BMDS weapons access, and complicates an enemy's ability to penetrate the defense system. In the terminal mode, the same radar provides surveillance, track, discrimination, and fire control support for the Terminal High Altitude

Area Defense weapon system. The AN/TPY-2 (FBM) system with the essential support equipment is shown in figure 2-5.

Figure 2-5. AN/TPY-2 (FBM) with essential support equipment

2-36. The AN/TPY-2 (FBM) system performs theater, medium, and long range search and target acquisition in support of strategic, regional, and theater missile defense missions. The AN/TPY-2 (FBM) system provides cueing data to Patriot, Terminal High Altitude Area Defense, Aegis ballistic missile defense (BMD), and GMD systems. The AN/TPY- 2 (FBM) system also has the capability to conduct collateral missions as directed by USSTRATCOM, including space surveillance and intelligence gathering. Refer to ATP 3-27.5, *AN/TPY-2 Forward Based Mode Radar Operations* for additional information on system operations and MDA Fact Sheet, Army Navy/Transportable Radar Surveillance (AN/TPY-2) for additional information on the AN/TPY-2 system.

COBRA DANE

2-37. The COBRA Dane radar located at Eareckson Air Force base on the island of Shemya, Alaska has been upgraded to include the missile defense mission and has been integrated into the BMDS. The upgrade improved GMD sensor coverage by providing acquisition, tracking, object classification, and data used for cueing, launch of interceptor missiles, and course updates of interceptors while retaining the site's legacy intelligence and space track missions. The Air Force has the responsibility for COBRA Dane system operations, maintenance, and sustainment. Refer to MDA Fact Sheet, COBRA DANE Upgrade for additional information on the COBRA Dane system. The COBRA Dane radar is shown in figure 2-6.

Figure 2-6. COBRA Dane radar at Shemya, Alaska

UPGRADED EARLY WARNING RADARS

2-38. Four Air Force operated early warning radars, located in Beale Air Force base, California; Royal Air Force Station Fylingdales, United Kingdom; Thule Air Base, Greenland; and Clear, Alaska were upgraded and integrated into the BMDS. The UEWRs have modernized hardware and software to improve GMD sensor coverage by providing critical early warning, tracking, object classification, and cueing data. The early warning radar in Cape Cod, Massachusetts began the UEWR modernization in FY13 and will be BMDS certified following the formal MDA ground test events. Refer to MDA Fact Sheet, Upgraded Early Warning Radars, AN/FPS-132 for additional information on the UEWR systems. The UEWR at Fylingdales, United Kingdom is shown in figure 2-7, on page 2-10.

Figure 2-7. Upgraded early warning radar at Royal Air Force Station Fylingdales

MARITIME DOMAIN

2-39. The sea-based x-band radar (SBX) and Aegis BMD make up the sea-based sensors which support the GMD Program. When deployed these sensors provide additional target acquisition and tracking allowing the GMD fire control operators to see more refined track data on the GMD fire control.

SEA-BASED X-BAND RADAR

2-40. The SBX is an advanced x-band radar mounted on a mobile, semi-submersible platform used to provide GMD with an extremely powerful and capable radar. The SBX may be positioned to provide coverage of any region of the globe. Its ocean-spanning mobility allows the radar to be repositioned as needed to support the various GMD test scenarios. The SBX is pictured in figure 2-8.

Figure 2-8. Sea-based x-band radar

2-41. The SBX radar acquires, tracks and discriminates the flight characteristics of ballistic missiles. The SBX provides an advanced capability to GMD, increasing the ability to conduct realistic testing of GMD, while providing an operational capability to the Combatant Commands.

2-42. The SBX provides an advanced radar capability to obtain missile tracking information while a threat missile is in flight. The radar provides discrimination between the missile warhead and penetration aids, and provides data to the EKVs so they may successfully intercept and destroy the threat missile before it reaches its target.

2-43. The SBX operates at sea for BMDS flight and ground test participation or in an active, operational status when indications and warnings signal the need for enhanced discrimination. The SBX is located in a Pacific port when not required at sea. The SBX maintains vessel certifications for operations at sea as well as software compatibility with the BMDS. Refer to MDA Fact Sheet, Sea-Based X-Band Radar (SBX) for additional information on the SBX system.

AEGIS BALLISTIC MISSILE DEFENSE

2-44. Aegis BMD is the naval component of the BMDS. The Aegis BMD weapon system is equipped with the AN/SPY-1, S-band phased-array radar system on the Navy Aegis Ticonderoga-class cruisers and the Arleigh Burke-class destroyers. Aegis ships concurrently provide long-range surveillance and tracking capability to support GMD engagements. An Aegis BMD destroyer is shown in figure 2-9, on page 2-12.

Figure 2-9. Aegis ballistic missile defense destroyer (DDG-70, USS Hopper)

2-45. Aegis BMD ships on ballistic missile defense patrol for homeland defense, detect and track ballistic missiles of all ranges – including ICBMs and report track data to the missile defense system. This capability shares tracking data to cue other missile defense sensors and provides fire control data to GBIs located at Fort Greely and Vandenberg Air Force Base and other elements of the BMDS including land-based firing units (Terminal High Altitude Area Defense, Patriot) and other Navy ballistic missile defense ships.

2-46. Planning for use of Aegis BMD to support homeland missile defense requires additional considerations compared to other BMDS elements. As a mobile multifunction maritime asset, there must be consideration for ship location, logistical support, air and missile defense protection, command, control, and mission priorities. Refer to MDA Fact Sheet, Aegis Ballistic Missile Defense for additional information on the Aegis BMD system.

COMMAND AND CONTROL, BATTLE MANAGEMENT, AND COMMUNICATIONS

2-47. C2BMC is the integrating element for BMDS to negate enemy ballistic missile threats, by providing critical mission coordination between BMDS sensors to weapon systems. C2BMC provides the foundation for conducting deliberate and crisis action planning for ballistic missile defense in accordance with JP 5-0, *Joint Planning*. It provides ballistic missile defense related situational awareness, sensor management, and battle management tools to allow operators to execute portions of the ballistic missile defense battle, and the global communications connectivity required to link all elements of the BMDS.

2-48. C2BMC is principally a battle staff tool and not a command execution tool. With the exception of AN/TPY-2 (FBM) sensor management, C2BMC provides specific situational awareness functions for the GMD community. C2BMC interfaces with sensor and weapon systems to establish a common operational picture of ballistic missile defense, detect threat missile launches, and enable the successful negation of those threats. C2BMC interacts with external elements to share information for more effective planning and to leverage non-BMDS resources to respond to threat situations. Refer to ATP 3-27.5 for additional information on the C2BMC system.

Chapter 3

Command and Control and Supporting Relationships

This chapter describes the command and control systems, United States Code authorities, relationships and responsibilities for the organizations involved in countering the global ballistic missile threat. The interorganizational relationships of these units is complex and includes the command authority. Lastly, this chapter describes the organizational structure of the GMD Units.

COMMAND AND CONTROL

3-1. Command and control is the exercise of authority and direction by the commander using mission orders to enable disciplined initiative within the commander's intent to empower agile and adaptive leaders in the conduct of unified land operations (ADP 6-0). The command and control warfighting function is the related tasks and systems used to develop and integrate those activities enabling a commander to balance the art of command and the science of control in order to integrate the other warfighting functions (ADP 3-0). This fundamental philosophy of command places people, rather than technology or systems, at the center. Under this philosophy, commanders drive the operations process through the activities of understand, visualize, describe, direct, lead, and assess. They develop teams of trusted Army professionals, both within their own organizations and with joint, interagency, and multinational partners. Commanders inform and influence audiences, inside and outside their organizations. It is this philosophy which allows us to focus less on the physical attributes of the defensive system and more on the command relationships and integrated operations.

3-2. An integrated strategy supports the rapid, flexible application of defensive capabilities synchronized with offensive actions is required to successfully exercise mission command, deter and defeat the enemy ballistic missile threat. This strategy is based on the principles of, unity of effort, unity of command, centralized planning, and decentralized execution.

3-3. USASMDC is the senior Army headquarters responsible for executing the GBMD mission. USASMDC forces will maintain a dedicated command structure to plan, integrate, and coordinate Army support to GMD. These capabilities will be part of a responsive, layered offensive and defensive system capable of deterring, preventing, or defeating missile threats as part of the greater GBMD mission.

3-4. The national command authority, combatant commands, and Service components are the organizations with a role in GMD. Army organizations with a have a role in GMD are USASMDC and the AAMDCs in their respective AORs. The Unified Command Plan identifies regional boundaries. However, since missile threats may cross AORs, combatant commands must coordinate to effectively counter missile threats.

3-5. By its very nature, ballistic missile defense is inherently joint and may be executed in multiple AORs simultaneously by the affected geographic combatant commanders. Consequently, all Services and many other organizations have key roles in ballistic missile defense. Because there are no overarching GBMD command structures, geographic combatant commanders use existing theater air and missile defense command organizations, such as area air defense commanders, AAMDCs, regional air defense commanders, and sector air defense commanders to conduct ballistic missile defense. Commanders must coordinate threat engagements which cross AOR boundaries.

GROUND-BASED MIDCOURSE DEFENSE COMMAND AND CONTROL SYSTEMS

3-6. Organizations with a role in GBMD utilize a wide range of ballistic missile defense battle management systems. These systems enable command relationships to mitigate complexities associated with cross-AOR operations. For GMD operations, these systems are C2BMC and the GMD fire control.

3-7. Command authority, USNORTHCOM, and geographic combatant commanders use the C2BMC system as a ballistic missile defense battle management decision aide. For GMD operations, the USNORTHCOM uses the GMD fire control for a decision aide and the Army utilizes the GMD fire control for fire control orders. The Army uses the C2BMC system for control of the AN/TPY-2 (FBM) radar system as well as an additional situational awareness tool.

3-8. Command relationships are the interrelated responsibilities between commanders, as well as the operational authority exercised by commanders in the chain of command; defined further as combatant command authority, OPCON, tactical control, or support.

3-9. Traditionally, command relationships are outlined through concept plans and operations plans, and are established and executed upon receipt of execution orders based on real threats. Increasing range and other technological advances in ballistic missiles may necessitate missile defense forces in one AOR to provide direct support to an adjacent combatant commander. The supported commander's requirements establish the overarching framework used by supporting commanders in their respective supporting plans. The supported commander's concept plan establishes the overarching framework used by AOR combatant commanders to develop supporting plans and to support regional missile defense plans.

3-10. Together, USSTRATCOM and JFCC-IMD, in coordination with USNORTHCOM, provide recommendations to the Joint Staff or Secretary of Defense to balance homeland defense requirements with the missile defense needs of other combatant commands. Supported by the Services, USSTRATCOM has the unique task of integrating missile defense requirements and Service capabilities across all AORs and linking GBMD planning with GMD Fire control execution.

3-11. At the operational level, the Joint Staff or Secretary of Defense establishes combatant commander relationships into supported and supporting roles. Balancing AOR priorities for defended assets with missile defense allocation in accordance with priorities set forth for homeland defense is challenging and requires participation from all combatant commanders.

3-12. The supported combatant commander, commander, USNORTHCOM, issues guidance for all facets of the GMD mission. The Army component provides forces to combatant commander to execute the GMD mission.

3-13. The Secretary of Defense will assign or attach forces to respective geographic combatant commanders as required for GBMD operations. The Secretary of Defense has directed the 100th MD BDE (GMD) and 49th MD BN (GMD) crews be OPCON to USSTRATCOM during day-to-day operations and will be OPCON to USNORTHCOM for combat operational execution. AN/TPY-2 (FBM) radars fall under the OPCON of the appropriate combatant command.

3-14. USNORTHCOM is the supported combatant command for homeland defense and directs engagement operations for active defense when the threat is to the United States, its territories, and its possessions. USNORTHCOM is the supporting combatant command for ballistic missile threats to other combatant commands. See figure 3-1 for an outline of GMD command relationships.

TITLES 10 AND 32 UNITED STATES CODE AUTHORITIES

3-15. Combatant commander for the GMD mission is commander, USSTRATCOM. GMD forces are assigned to USSTRATCOM through USASMDC. OPCON of the GMD mission transitions to USNORTHCOM for the defense of North America during mission execution. All GMD units fall under the OPCON of either USASMDC or USNORTHCOM depending on the current operational posture.

3-16. The authority and procedures for staffing the GMD sites and performing the Federal GMD operational mission utilizes Active Army, dual-status ARNG commanders, and ARNG AGR Soldiers. This authority is

contained in the Secretary of the Army approved GMD staffing model, the standing USASMDC general order, and the memorandum of agreement between the National Guard Bureau, USASMDC, and the states of Colorado, California, and Alaska. GMD commanders exercise full command authority over their respective commands. Federal and state agencies are involved in the GMD mission and their respective chains of command are separate and distinct and should not be confused. The command

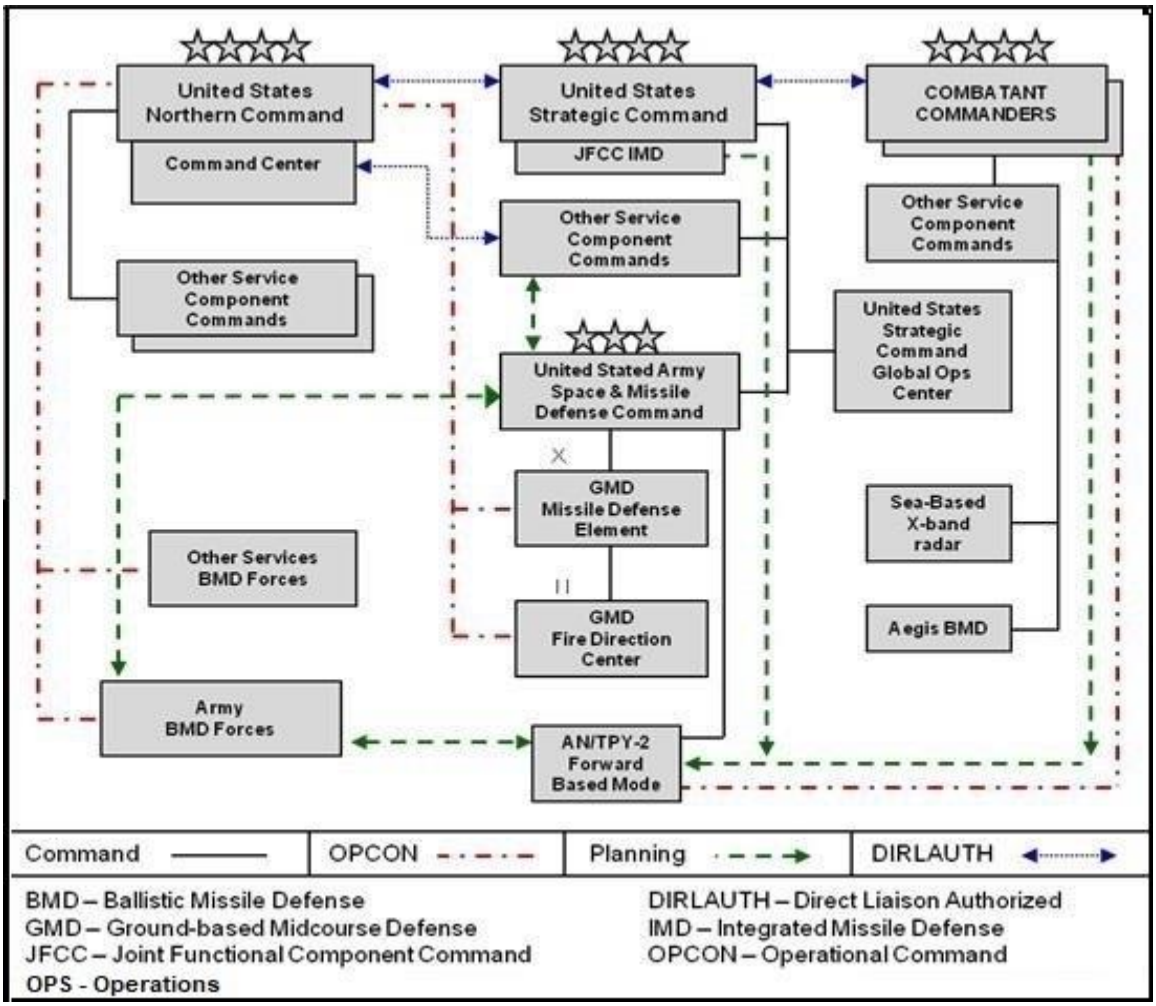

Figure 3-1. Ground-based Midcourse Defense command relationships

3-17. The 100th MD BDE (GMD) Commander is a Title 10 and Title 32 dual-status commander. While acting within Title 10 authority, the 100th MD BDE (GMD) commander has command authority over all Title 10 Soldiers from Colorado, Alaska, and California performing the GMD mission. While acting within Title 32 authority, the 100th MD BDE (GMD) commander has command authority over only those Soldiers from Colorado.

3-18. GMD operators will remain under the control of the established Title 10 United States Code, Title 32 United States Code, or Title 50 United States Code chain of command when conducting missile defense operational duties. The Secretary of Defense, as the President's principal assistant on military matters, has overall authority for DOD and executes the homeland defense mission (JP 3-27). Colorado, California and Alaska ARNG Soldiers executing the GMD mission or guarding the GMD facilities do so only while in a Title 10 status and under the command of the Title 10 chain of command.

3-19. GMD Soldiers in a Title 32 status are under the command of their state ARNG chain of command to include administrative and disciplinary authority. GMD Soldiers in a Title 10 status fall under the administrative and disciplinary authority of their Title 10 chain of command, the 49th MD BN (GMD) and 100th MD BDE (GMD).

3-20. AGR Soldiers transition to Title 10 status upon entering the GMD operational site or otherwise upon order of the Title 10, chain of command. Soldiers return to Title 32 status when released from Federal service, when released by their Title 10 chain of command, or when they have departed the GMD operational facility where they were performing Title 10 duties.

COMBATANT COMMANDS

3-21. Combatant commands are joint military commands composed of forces from two or more Services, have a broad and continuing mission, and are organized either on a geographical basis or on a functional basis. All combatant commands are commanded by either a four-star general or admiral and are considered joint commands with specific badges denoting their affiliation.

3-22. As directed, combatant commands provide support to the commander, USNORTHCOM for missile defense of the US homeland to include the territories. For example, Commander, United States Indo- Pacific Command is the supporting commander to commander, USNORTHCOM for execution of the GMD mission with Aegis BMD ships and AN/TPY-2 (FBM) track data for ICBM threats to the homeland (sea, land, and space-based).

3-23. USNORTHCOM is the supported geographic combatant commander for homeland defense and directs active defense engagement operations when the threat is directed to the United States, its territories, and its possessions. USNORTHCOM is a supporting geographic combatant commander for ballistic missile threats to other geographic combatant commanders.

3-24. The AN/TPY-2 (FBM) system has cross-AOR capability, which may result in radar taskings in support of multiple combatant commanders. The desired outcome of cross-AOR planning includes:

- Identifying and planning information exchange requirements and links between all users of the radar data are included in the regional C3 architecture;
- Sensor management requirements identified for cross-AOR multiple mission sensors;
- Cross-AOR mission and taskings are codified in support plans, operations orders, Execution Orders, or appropriate command agreements;
- Defense plans codified in the combatant commander training plans, exercises, and Defense Readiness Reporting Systems;
- Assigned missions with cross-AOR boundaries and support defense against multiple AORs; and
- Direct support relationships established between geographic combatant commanders to define the supported commander's requirements.

3-25. The AN/TPY-2 (FBM) systems are OPCON to the assigned geographic combatant commander who is the supported commander in a regional defense situation. The geographic combatant commander with OPCON of an AN/TPY-2 (FBM) system is the supported commander in a theater mission, and is in a supporting commander role to the commander, USNORTHCOM in the conduct of the homeland defense mission. There are situations where a geographic combatant commander may simultaneously be the supported and supporting commander. The geographic combatant commander may use the AN/TPY-2 (FBM) system to concurrently support both regional and strategic missile defense operations. Before deployment of an AN/TPY-2 (FBM) system into a theater of operations, command and execution authority must establish clear lines of authority during crisis operations for concurrent strategic and regional operations.

ARMY NATIONAL GUARD RESPONSIBILITIES

3-26. AGR Soldiers who transition from Title 32 to Title 10 status in order to execute the Federal GMD mission, in accordance with the Secretary of the Army approved staffing model provides the majority of the staffing for Army GMD elements. A mixture of Active Army and AGR personnel provide the MDE with sufficient personnel to execute the continuous GMD mission. Crews at the MDE and FDC will conduct operations under the OPCON of USNORTHCOM.

3-27. Staffing is a mix of Active Army, ARNG AGR, Department of the Army Civilians and contractors. Thus, the concept of operations is complex. USASMDC is the senior Army headquarters responsible for executing the GMD mission and executes the Title 10 Federal mission. The 100th MD BDE (GMD) is aligned

with the Colorado ARNG, Detachment 1 is aligned with the California ARNG, and the 49th MD BN (GMD) is aligned with the Alaska ARNG. The BDE and BN commanders are dual-status, serving in both a Title 10 and Title 32 capacity. AGR Soldiers executing the GMD mission or guarding the GMD facilities do so only while in a Title 10 status and under the command of the Title 10 chain of command.

GOVERNOR AND ADJUTANT GENERAL RELATIONSHIP

3-28. Governors, acting through their Adjutant General, exercise mission command over their state ARNG forces. As members of the ARNG, the dual-status commanders take Title 32 orders from the Governors, through the Adjutants General of their respective states. Governors and their Adjutants General understand the Title 10 GMD mission has precedence over all other missions, at all times. The exercise of state command authority shall not conflict with the GMD mission. Adjutants General retain authority over the ARNG units and Soldiers only when in a Title 32 status. The state Adjutant Generals have no command authority over the Soldiers of the 100th MD BDE (GMD) or 49th MD BN (GMD) when in Title 10 status.

3-29. The supported combatant commander for the GMD mission and the commander of USASMDC provide federal control over GMD forces performing Title 10 duties. The dual-status commanders, as Federal officers performing active duty under Title 10, take orders from the President or those officers the President and Secretary of Defense have authorized to act on their behalf.

3-30. The command and support relationships of the Soldiers performing the GMD mission are complex and dynamic, as indicated in figure 3-2.

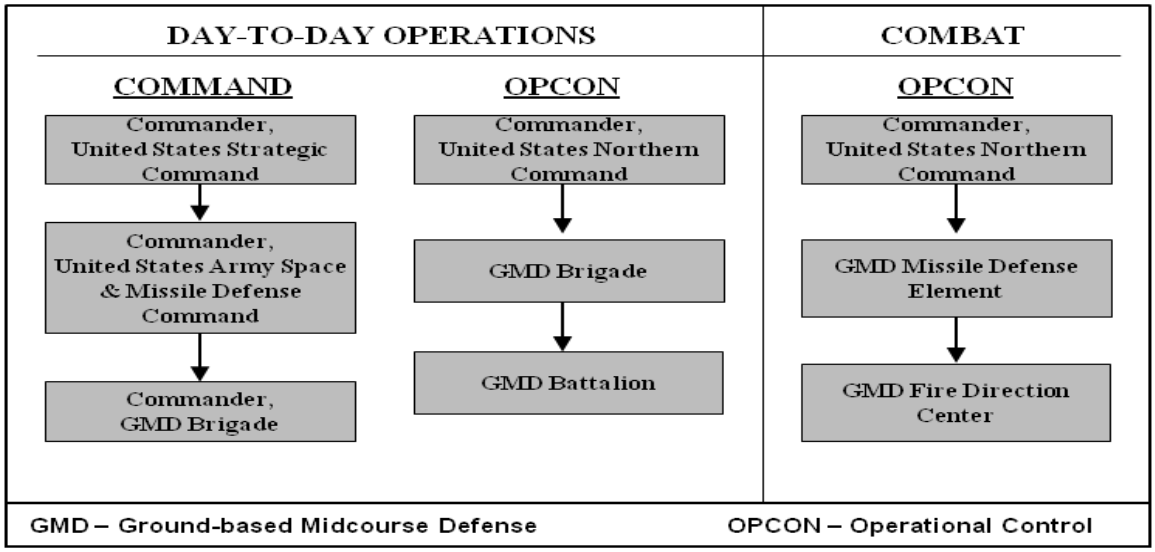

Figure 3-2. Command relationships

3-31. The Adjutants General are responsible to provide personnel for ARNG units. The Adjutants General must plan the activation, support, and recruitment of the personnel to staff the GMD units. Responsibilities include:

- Providing personnel management for AGR Soldiers working the GMD mission;
- Providing training for AGR Soldiers working the GMD mission to be proficient in their common Soldier, individual military occupational specialty tasks, and required tasks unique to the AOR; and
- Ensure Title 32 Soldiers perform Title 32 AGR duties when not performing their Federal mission. AGR Soldiers in Title 32 duty status organize, administer, recruit, instruct, or train the reserve components. Duty descriptions of Title 32 AGR Soldiers will reflect these duties the Soldier performs on a regular basis.

ORGANIZATIONAL STRUCTURE

3-32. The USASMDC exercises administrative control and responsibility of the GMD units and serves as the combat developer for the GMD system while the National Guard Bureau and the state Adjutants General of Alaska, California, and Colorado provide general equipment and personnel who transition to a Title 10 status in order to staff the operational nodes. GMD unit leaders and operators are members of the Army space cadre because they execute a space force application mission and leverage multiple space enabling capabilities. The Army defines its space cadre as space professionals and space enablers. Space professionals are career space specialists, who plan, develop, resource, acquire, integrate or operate space forces, concepts, application or capabilities. Space enablers are Army personnel who perform unique space tasks or functions or may require specialized skills to apply space capabilities. Figure 3-3 provides an outline of the GMD organizational structure.

3-33. USASMDC oversees the Army's Title 10 United States Code mission. Army organizations involved in GMD operations include:

- 100th MD BDE (GMD) provides staffing for the MDE executing GMD operations;
- 49th MD BN (GMD) provides staffing for the FDC executing GMD operations;
- Detachment 1 at Vandenberg Air Force Base;
- Fort Drum Security Detachment;
- Future GMD Detachments; and
- Theater missile warning, defense planners, and units outside the continental United States.

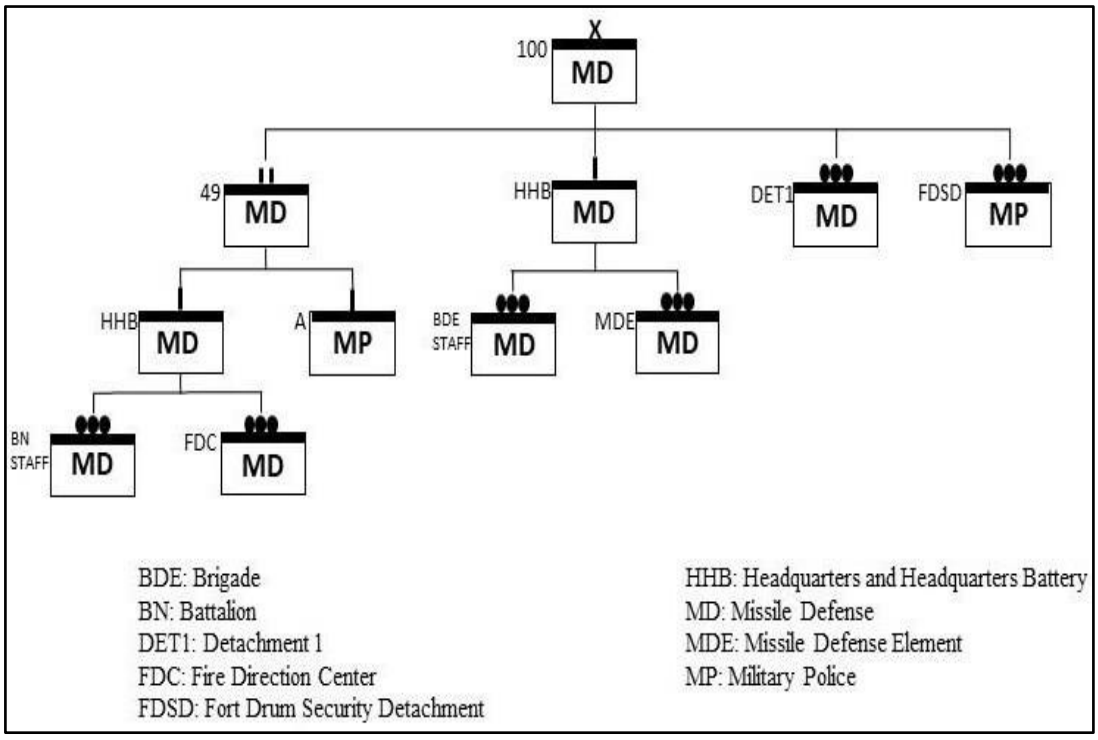

Figure 3-3. Organizational structure

Chapter 4

Fire Control Operations

This chapter presents an overview of operations and considerations GMD units must apply for the planning and execution of their mission. This chapter also describes the training and exercise capabilities within the command and the GMD fire control system itself.

SECTION I – GROUND-BASED MIDCOURSE DEFENSE ENGAGEMENT OPERATIONS

4-1. This section discusses the planning and engagement criteria which must be considered for GMD engagement operations. This sectional also outlines an example of a nominal GMD engagement sequence.

OPERATIONS PLANNING

4-2. USSTRATCOM, through the JFCC-IMD, conducts centralized planning for GBMD and coordinates with USNORTHCOM for planning related to GMD operations. USNORTHCOM defines all engagement criteria according to threat capability parameters, commander's intent, and national security objectives within their AOR. Service components conduct the detailed planning to maximize Service capabilities.

4-3. GMD operational planning is linked with the planning of other BMDS capabilities used to engage ballistic missiles capable of striking targets within the United States. A critical element of operational planning is the establishment of the combatant prioritized critical asset list and creation of the defended asset list. Locations and priority of assets on the defended asset list affect the configuration of the GMD system's defensive task plans.

4-4. Like all military operations planning, GMD commanders and planners use the standard military decision-making process which should include prudent risk assessment (see ATP 5-19) and acknowledgement of ethical considerations as expressed in the moral principles of the Army ethic. The key part is the commander's intent. GMD planners must always keep their commander's intent foremost as they develop GMD battle plans for the various engagement scenarios. The battle plans require delineation of a geographic defended areas and input of DS/XP data and control parameters to establish or limit the system's operations. Operators and planners must determine DS/XP factors and decide how to implement other military or civil controls or restraints without a built in hardware or software mode of execution.

4-5. GMD has a capability for multiple XPs. XPs are developed in accordance with the commander's intent to address several probable event sequences. Once a DS/XP is selected, operators must fully understand the GMD system response to the commander's intent.

ENGAGEMENT CRITERIA

4-6. Engagement criteria are critical elements of planning. A competent authority issues engagement criteria directives to delineate the circumstances and limitations under which United States forces initiate and continue combat engagement with other forces. The Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 3121.01B, *Standing Rules of Engagement/Standing Rules for the Use of Force for US Forces* provides fundamental policies and procedures governing the actions of commanders and Soldiers during all military operations. For GMD, the engagement criteria are defined by USNORTHCOM and these must be met before a determination will be made to release GBIs. Procedurally, the engagement criteria must be met before the GMD fire control crew director requests permission to place the GMD fire control into a weapons free state. The weapons release authority (known as WRA) will grant permission to place the GMD system into a weapons free state and will authorize engagement against each threat individually.

4-7. Supplemental rules may augment the standing ROE and rules for the use of force. Approval of supplemental ROE and rules for the use of force in accordance with CJCSI 3121.01B is necessary before issue. Supplemental engagement criteria are always applicable unless superseded by properly approved and directed supplemental ROE and rules for the use of force. Other directives issued by the President, Secretary of Defense, or other competent authority, such as those delineating weapons free, may modify or supersede provisions in the standing ROE.

ENGAGEMENT OPERATIONS

4-8. Army forces must acquire and fuse a constant flow of situational awareness data and information. Missile defense forces use approved tactics, techniques, and procedures. Although planning and engagement authorization is centralized, effective engagements require decentralized execution. In order to conduct decentralized execution, the GMD crews have to know the commander's intent for engaging a threat before the crews begin a battle. Crew members receive the commander's intent from the commander in the form of concept plans, concept of operations, operations orders, and fragmentary orders. The speed at which attacking ballistic missiles travel and the range and the speed at which GMD intercepts occur makes rapid responses essential for a successful engagement. GMD execution uses automated processes with specific human-in-control functions.

4-9. Overhead persistent infrared sensors, which includes the SBIRS constellation, should provide the first indication of a ballistic missile launch. These sensors should also provide the first indication of a ballistic missile launch threatening the defended areas. The overhead persistent infrared sensors will continue to track the missile until booster burnout. GMD operators track the launch throughout its trajectory based on data received from overhead persistent infrared space-based, ground-based, and sea-based data collection platforms, providing greater fidelity on predicted impact. Once a determination is made the engagement criteria have been met, the weapons release authority authorizes weapons free, and the USNORTHCOM MDO passes weapons free authorization to the MDE crews who initiate an engagement sequence for each threat.

4-10. The automated battle management decision support portion of the GMD fire control capability will provide the commander, USNORTHCOM with the capability to assess the threat, characterize the attack, and provide force direction to best defend against the threat. The automated engagement planner provides essential fire control and other system information to the GMD operator enabling battle redirection in support of the commander's intent. The engagement planner uses sensor data and operator input to plan and build tasks for the GMD system to use when tracking objects, engaging targets, and providing the GBI and EKV guidance.

4-11. The AAMDCs conduct joint and combined integrated air and missile defense to support designated concept plans or operations plans. The AAMDCs supports GBMD operations with the AN/TPY-2 (FBM) radars within their AOR in accordance with guidance from the combatant commands. The AN/TPY-2 (FBM) radar sensor management section operates the C2BMC system in the employment of the AN/TPY-2 (FBM) radar and is integrated with the AAMDC. This integration normally occurs at the joint air and space operations center supporting the combatant command.

4-12. Overhead persistent infrared, AN/TPY-2 (FBM), and Aegis BMD provide launch location, initial track data, early warning, target type-classification, fire control data, sensor cueing data, and target impact-point estimates to the GMD fire control. The GMD fire control uses additional data from COBRA Dane, UEWRs, SBX (if available), AN/TPY-2 (FBM), and Aegis BMD to determine state vectors (grouping of six mathematical values to describe the three-dimensional location, direction, and speed of an airborne or space borne object in relation to the Earth's surface), determine a predicted impact point, assess the threat to the defended areas and alert GMD systems. The human-in-control determines whether engagement criteria are met and enables further actions. Figure 4-1 is a graphic illustration of GMD system engagement and Table 4-1 (page 4-4) provides detailed events for the GMD engagement sequence.

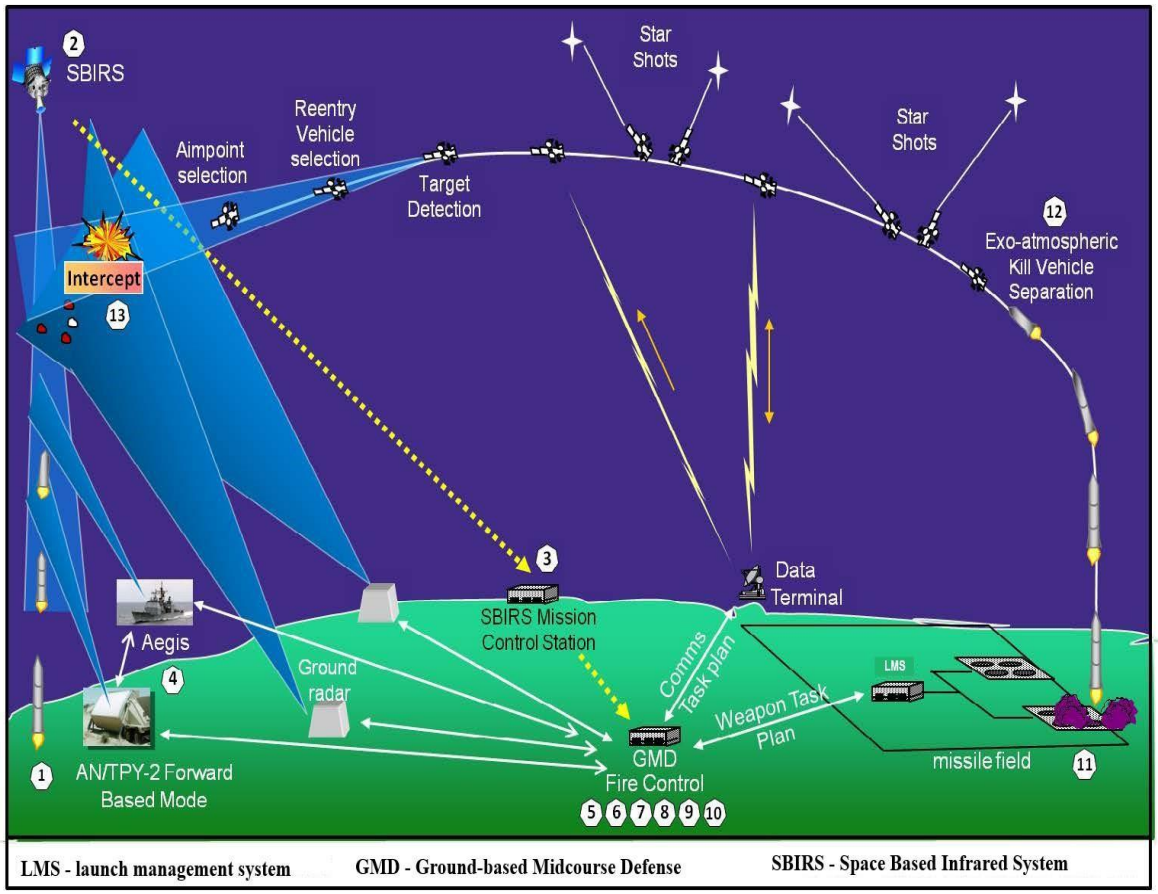

Figure 4-1. Example engagement sequence

4-13. When the MDE and FDC operators confirm the GMD fire control automated recommendations and verify engagement criteria are met, they will request a change in weapons control status to weapons-free authorization for engagement. The GMD fire control engagement planner builds and sends a Sensor Task Plan to cue sensors to begin tracking the threat objects providing additional situational awareness to the operator. Surface sensors detect the threat objects once they enter the radars' range and field of view. Some forward based sensors may detect missile launches in the boost phase, if appropriately located.

4-14. Space-based and surface sensors detect the ballistic missile as it enters the sensors field of view. With initial sensors input from Overhead Persistent Infrared, Aegis BMD, and the AN/TPY-2 (FBM) radar, the GMD fire control begins building a fire solution. COBRA Dane, UEWR radars, and SBX continue to track and refine data used by the GMD fire control in launching the GBI. The refined data is sent to the EKV to guide it to the target.

4-15. GMD operators will monitor the threatening missile's trajectory. The GMD fire control establishes a track file and provides an assessment with options to the operators. Operators must visualize the battle to decide:

- Predicted impact points;
- Determine if the event is a threat;
- Number and engagement timeline of incoming RV to engage;
- Execute pre-approved firing guidelines; and
- Pattern and time between launches.

Table 4-1. Example GMD engagement sequence

STEP	*EVENT*
1	Threat intercontinental ballistic missile launches.
2	Space-based infrared system satellites detects the launch and pass infrared data to the space-based infrared system mission control station.
3	Mission Control Station passes threat data to the GMD fire control and C2BMC systems, alerting missile defense element and fire direction control centers.
4	The AN/TPY-2 forward-based mode radars and Aegis BMD ships acquire and begin tracking the threat intercontinental ballistic missile. Track data is passed to the GMD fire control system.
5	Once the GMD fire control determines there is a threat to the defended area, the system transitions to system state alert and sends a message to all GMD assets. Crew members may manually transition the GMD fire control to alert as well.
6	When crews determine the rules of engagement have been met, they request weapons free from the weapon release authority.
7	GMD fire control uses radar data to cue additional radars, so they may more rapidly acquire the threat.
8	If the GMD fire control needs to launch GBIs, it has enough data at this time (if system is enabled with weapons free and GBIs are available); however, the GMD fire control system prefers higher resolution of the threat, so if weapons access is available, the GMD fire control may wait until it identifies the reentry vehicle before committing and launching the GBI against the threat. This higher resolution data comes from the sea-based x-band radar if it is in position.
9	The crews evaluate the threat and determine the proper GBI allocation to meet the commander's intent per threat and apply them in accordance with their firing doctrine.
10	Shortly before the GMD fire control decides to launch a GBI, the GMD fire control system sends out a defend integrated task plan, which consists of sensor task plan – requesting specific information from radars to support the intercept, communication task plans – tasking specific in-flight interceptor communications system to support communication events between the GMD fire control system and the EKV, and a weapons task plan – providing specific targeting information to the GBI dedicated to the intercept.
11	Shortly after receiving the weapons task plan, the GBI launches; at launch, the GBI has the information it needs to make a successful intercept of the threat, however, the GMD fire control system has the ability to send in-flight target updates to the EKV, so the EKV has the most refined threat picture prior to making the intercept.
12	After the GBI launches and the booster completes its burn, the EKV separates and completes star shots to verify its location. The EKV then maneuvers to receive communications event 1, which consists of an in-flight target update and transmission of an in-flight status report (which lets the GMD fire control know the status of the EKV). It makes course corrections with the information from the in-flight target update then maneuvers to receive communications event 2 which consists of an in-flight target update only.
13	At a predetermined range, the EKV acquires the threat complex. With the use of its on-board sensors, the EKV determines which object is the reentry vehicle and directs itself into the reentry vehicle destroying it by force of impact or kinetic energy.
14	Threat intercepted. If tasked, sea-based x-band radar may provide a hit assessment. This process is repeated for all threats until the battle is over or the GMD system is out of inventory.

BMD – ballistic missile defense
EKV – exo-atmospheric kill vehicle
GBI – ground-based interceptor
GMD – ground-based midcourse defense

4-16. During tactical operations, operators should strive to select options to enhance flexibility, preserve the ability to identify off-nominal situation possibilities, and retain their ability to respond to these situations in later phases of the threat's flight. Some illustrative tasks which retain flexibility, with permission, are:

- Adjust the allocation of GBIs against each threat to account for off-nominal situation and ensure the commander's intent is met;
- Monitor targets for validity, change in identification, splitting, and emerging new threats; and
- Battle redirection – reallocation of GBIs to meet commander's intent.

4-17. Interceptors may be launched individually or in salvos (multiple GBIs) per target as determined by the GMD fire control. The method of fire is based on the operator's configuration of the GMD fire control system to allocate GBIs based on the threats, tactics, techniques, and procedures, and the fire control orders input manually to change the GBI allocation. The basis of GBI allocation and sequencing of launch are based upon several factors. These factors include data available in the GMD fire control, the crew and director's interpretation of the situation, and their determination of how to best meet the commander's intent to determine how many GBIs are launched and when.

4-18. The DS/XP is based on pre-defined commander's intent and contains the battle plan and GMD fire control system configuration. The DS/XP contains the parameters the GMD fire control uses to determine the threat and the number of GBIs to automatically allocate to satisfactorily engage the threat. Human-in-control capabilities allow real-time, battle changes to meet the commander's intent and Presidential guidance or Secretary of Defense-level pre-approved firing guidance as the battle evolves. Due to the short timeframe to defend against a ballistic missile attack coupled with the fixed GBI locations, a pre-determined DS/XP is used to determine the minimum number of missiles for each engagement, but the GMD fire control operator provides oversight and intervention of the GMD battle to ensure the commander's intent is met for each threat engagement.

READINESS CONDITION

4-19. In planning, increased contingency security should be married to both missile defense readiness condition and force protection conditions to account for both the mission criticality of the assets being secured and the threat against them. Security augmentation should be considered during contingencies, increased readiness condition and increased force protection condition. Readiness condition information may be found in the USSTRATCOM Strategic Instructions.

4-20. USNORTHCOM, the 100th MD BDE (GMD) and 49th MD BN (GMD) ensure GMD elements are operationally ready according to the potential for attack, the threat level, force protection condition, and the readiness condition. All systems must be ready to complete assigned missions, while managing many factors, such as routine maintenance, weather, training, and equipment upgrades.

SECTION II – TECHNIQUES

4-21. This sections discusses different techniques employed by the GMD fire control operators.

EMPLOYMENT GUIDELINES

4-22. The GMD employment guidelines are to assist GMD fire control operators in meeting the commander's intent. The GMD employment guidelines represent the best case application of combat power, and they represent the optimal way of utilizing the GMD system. The GMD employment guidelines are:

- Understand the commander's intent;
- Visualize the operational environment;
- Select the best GMD fire control DS/XP;
- Retain flexibility; and
- Maintain situational awareness.

UNDERSTAND COMMANDER'S INTENT

4-23. This guideline focuses on developing a thorough understanding of how the commander is responsible for the GMD fight, and how the commander wants the GMD fire control operators to fight the GMD battle. Every member of the GMD crew must understand the commander's intent prior to assuming a shift on an

operational system, because the operational crews must be prepared to react immediately to an ICBM launch against the designated defended areas.

4-24. Key tasks associated with this employment guideline are:

- The GMD operators must conduct a thorough mission analysis to understand the commander's intent and guidance for the GMD fight;
- Translate the commander's intent and guidance into requirements on how to configure the GMD system, which tells the system how to allocate interceptors against threats;
- Understanding the commander's intent for the system DS/XP against ICBM threats to the defended areas. All changes to the system configuration authorized for implementation during the course of the battle are necessary to meet the commander's intent for missile allocation; and
- Understand all the situations the GMD operator will have to face in order to achieve the commander's intent.

VISUALIZE THE OPERATIONAL ENVIRONMENT

4-25. Critical to GMD employment is visualization of the operational element as it relates to the threat and its current capacity to target the defended areas. GMD operators visualize the battle through analysis of information provided by the GMD fire control communications and through information and intelligence provided by the Joint community. By understanding the threat, GMD operator's best decide the appropriate allocation of interceptors to react to the incoming threat. Understanding the ability of the system to deal with the threat, the GMD operators must identify key decision points during each engagement.

SELECT THE BEST BATTLE PLAN

4-26. Battle plan analysis takes place throughout the battle providing the GMD operator with the flexibility to conduct battle redirection if necessary. The GMD fire control battle plan is the mission directives the operators enter into the system to allow the GMD fire control to fight the threat according to the commander's intent. The DS/XP consists of the following four mission directives:

- Defended area - A geographical area, which defines for the GMD fire control what to defend;
- DS/XP - Values defining interceptor allocation, such as cut-offs and thresholds and defended asset list, by category, in the defended areas;
- Mission constraints - Control parameters refining interceptor allocation and engagement execution against a threat; and
- Reserve - Control parameters restricting interceptor availability against a threat.

4-27. Once the GMD operators understand the threat, they must decide if the current system configuration is going to be effective in fighting the threat they face. For example, the operators must understand if the automated allocation system allows them to effectively meet the commander's intent for allocation against the current threat. This requires continual analysis throughout the entire GMD battle and the GMD fire control operators may change the automated interceptor allocation and reconfigure specific system parameters at any time during the battle.

RETAIN FLEXIBILITY

4-28. Various DS/XP settings enable the GMD operator to retain flexibility throughout the engagement sequence. This guideline includes all actions associated with battle redirection actions applied to inbound threats on a case-by-case basis. The GMD operator will adhere to this GMD employment guideline. Operators recommend all management-by-exception actions based on shot doctrine associated with manipulating the automated missile allocation based upon a track-by-track analysis and accounting for any near term future threat.

4-29. GMD operators evaluate each threat and determine if they are correctly implementing the commander's intent. If not, they will manipulate the allocation so the commander's intent is met. When accounting for the near term, future, or follow-on threats, the GMD fire control system only fight threats it sees. It is up to the GMD operator, with guidance from higher headquarters, to determine if retaining a portion of the available interceptors is necessary for future allocation against near term future threats.

MAINTAIN SITUATIONAL AWARENESS

4-30. The purpose of GMD employment guidelines is to maximize situational awareness for the GMD operator throughout the fight. Through careful consideration of all the guidelines combined, the operator not only gains situational awareness of immediate actions at the tactical level, but also maintains greater awareness of guidance derived from operational and strategic leaders. The same is true for the GMD system; the GMD fire control operator must maintain a constant awareness of the GMD system's capabilities, as it will determine how an operator will utilize the system during the battle.

FIRE CONTROL

4-31. The GMD fire control system offers many options allowing the operators to manipulate the system in order to best meet the commander's intent.

MANAGEMENT BY EXCEPTION

4-32. The GMD fire control was designed to operate autonomously. However, the desire to keep humans in the loop required a method to manage the system effectively. The principle of management by exception was developed to keep humans in control of the system and reinforces the concept no one commander may direct the overall missile defense operation on a real-time basis. Management by exception is the standard method of fire control for GMD operations to ensure proper fire distribution and to meet the commander's intent.

HEALTH AND STATUS REPORTING

4-33. The Resource Status Window indicates changes of status from sensors to mission operators. Operators monitor the health and status of resources in order to relay this information to USNORTHCOM and to best meet the commander's intent as they engage threats.

GBI INVENTORY MANAGEMENT

4-34. Commander's guidance should establish interceptor inventory threshold levels at which operators may need to modify firing procedures to prevent premature inventory exhaustion and proper allocation of interceptors. Close coordination between the MDO and crew directors should be maintained to ensure commander, USNORTHCOM and the weapons release authority are aware of GBI inventory.

POSITION SELECTION

4-35. All operators work from one of six workstations. Although dedicated positions for each crewmember are established, crewmembers may log into the system and select any operator position from any workstation. This is essential if a workstation becomes non-functional and a crewmember is forced to relocate to the surge position.

MISSION DIRECTIVES

4-36. There are two different classes of directives which may be manipulated, GMD and GMD fire control. The GMD directives require the GMD fire control to issue changes and tasking messages to external resources and include system state and weapons control. The GMD fire control directives affect the GMD fire control components and include ROE, weapons control, DS/XP, mission constraints, reserve, manage by exception, terminate engagement, defended area, and readiness condition. These directives allow the operators to manipulate GMD assets and the GMD fire control system in order to engage threats in the manner which best meets the commander's intent.

TOKEN CONTROL

4-37. A token is used as an electronic identification method within a multi-node configured suite to identify the lead server for transmission of track data to ensure all linked terminals receive and display the same track information. The token may be transferred between nodes to maintain positive integrity of track data. The

token methodology also applies within a single node, but the token remains within the single node. The token generally resides at the node with the least degradation.

WEAPONS CONTROL STATUS

4-38. Weapon control status describes the control of fires and applies to the GMD fire control for release of GBIs. The weapons control states of the GMD fire control elements will be directed by the weapons release authority. There are two weapon control statuses.

- Weapons free. Weapons release authority has been granted for specific threat tracks and weapons task plan are generated and sent to the LMS. GBIs are capable of launching once removed from a reserve status. This is the least restrictive weapon control status.
- Weapons hold. Weapons task plan are not being sent to the LMS and the GBIs are incapable of launching. This is the most restrictive weapon control status.

RULES OF ENGAGEMENT

4-39. ROE are the means to provide military commanders guidance for weapons employment consistent with law and policy. ROE are procedural management directives to specify the circumstances under which GMD operators initiate, or to continue to initiate combat engagements. ROE also prevent engagements when the criteria are not met. The ROE are approved during planning stages and updated as required, to remain consistent with commander's intent before engagement begins. Supporting legal advisors can provide advice on ROE during the planning stages. These established ROE enable the GMD fire control elements to prescribe the exact condition of engagements. Due to short engagement timelines associated with ballistic missile flights, ROE must be well known by all members in the fire control chain of command, thoroughly trained, and regularly practiced during exercises.

FIRE CONTROL ORDERS

4-40. Fire control orders are established to standardize tactical firing instructions issued during the conduct of battle and are commands used to control engagements on a case-by-case basis. Fire control orders are transmitted verbally over the GMD Link. There are three fire control orders used by the GMD fire control elements.

- Weapons free. This command directs or authorizes the fire control nodes to engage a designated target. This order must be provided for each target.
- Cease fire. This command directs the fire control nodes to stop the firing sequence against a designated target, however, interceptors already in flight are permitted to continue to intercept.
- Hold fire. This command is an emergency order used to stop firing. If technically possible, interceptors already in flight must be prevented from intercepting.

USE OF SALVOS AND SALVO SIZE

4-41. Depending on the threat launch locations, launching multiple interceptors may increase the probability of an intercept. Multiple threat launches may prevent repetitive kill evaluations and re-engagement decisions. The more time a threat missile spends in the midcourse phase, the greater the possibility it may deploy countermeasures and penetration aides, if equipped. Similarly, the GMD sensors have more time to discriminate the RV from countermeasures, penetration aides, chaff, and other objects along the same trajectory.

4-42. Interceptors may be launched individually or in salvos at each target as determined by the operators and the GMD fire control system. The use of salvos as method of fire is based on the operator's configuration of the GMD fire control system to allocate GBIs based on the commander's intent; the specific threat; tactics, techniques, procedures; and the fire control orders manually entered to change the GBI allocation. GBI allocation and sequencing of launch are based upon many factors. These factors include data available in the GMD fire control, the crew's interpretation of the situation, and their determination of how to best meet the commander's intent.

TRAINING AND EXERCISES

4-43. In order to maintain proficiency on the GMD fire control system, operators conduct regular training and undergo routine certifications. In addition, the GMD fire control allows operators to conduct real world operations concurrently with tests and distributed exercises.

GUNNERY PROGRAM

4-44. The commander, USASMDC has the responsibility to develop and maintain certified GMD and AN/TPY-2 (FBM) operators for the combatant commanders. The goal of the gunnery program is standardization and performance proficiency of GMD operations for all crewmembers and crews. Therefore, prior to standing GMD crew duty, all GMD operators will successfully complete the individual training and evaluation requirements.

4-45. There are three levels of gunnery tables for GMD operators:

- Basic is used to train individuals to perform as crewmembers;
- Intermediate is used to train crews to operate collectively; and
- Advanced is used to train crews to operate collectively under increasingly difficult circumstances.

CONCURRENT TEST AND OPERATIONS

4-46. Concurrent test and operations distributed multi-echelon training system consists of live, virtual and constructive training environments allowing for proficiency training, operator certification, wargames and exercises, and tactics, techniques and procedures development, review, testing and revision. The concurrent test and operations distributed multi-echelon training system has the ability to create wargame-like environments for units to conduct training or other objectives by presenting standardized, technically accurate threat scenarios, problems, faults, and situations to elicit the performance of an individual or crew. As the material developer continues to develop the BMDS, the development of concurrent test and operations distributed multi-echelon training system will keep pace with an ability to effectively train the crews, elements, staffs, and commanders who execute the evolving GMD mission.

This page intentionally left blank.

Chapter 5

Communications

This chapter describes the global communications systems needed to support GMD and provides a general review of the existing architectures in support of global communications. The global communications network, which is part of the Department of Defense information network (DODIN), connects GMD elements with fire control networks for missile intercepts. Additionally, key organizations who support GMD have duties and responsibilities to ensure specific communications systems and equipment are always available to support GMD mission command and battle management.

OVERVIEW

5-1. GMD uses many secure voice and data communication systems to execute the mission. The GMD communications capability will be secure, interoperable, collaborative, redundant, and survivable to provide connectivity to the entire GMD community. Cybersecurity must be built into every aspect of the system to ensure a high probability of mission success.

COMMUNICATIONS REQUIREMENTS

5-2. Reliable communications are imperative for GMD systems conducting their mission. Effective battle management requires reliable communications support to enable the commander to conduct operations during stressing situations, for prolonged time periods, over vast distances. The commander must retain the flexibility to maintain communication links with the mission command elements, space-based systems, and to maintain access to time-sensitive data to effectively conduct operations.

5-3. GMD Communications systems require the capability to collect, process, display, and communicate large amounts of information while denying the enemy access to the information. Communications systems supporting GMD, including space-based resources, are capable of providing secure near real-time exchange of essential information between the GMD fire control and the external assets. The systems must be sufficiently flexible and responsive to allow timely redirection of GMD resources. GMD communications systems must have sufficient capacity, electronic protection, and flexibility to accommodate information exchange even when operating at degraded levels.

GROUND-BASED MIDCOURSE DEFENSE NETWORKS

5-4. To support GMD operations, communications are established and maintained using all available means, including strategic, tactical service component, sustaining base, and commercially-leased communications. The required communications must support high-speed data systems with massive data storage, retrieval, and dissemination capabilities. The following types of information are exchanged:

- Situational awareness – consisting of the common operational picture, alerting, and early warning;
- Command and control– consisting of command, OPCON, and tactical control;
- Operations and intelligence – consisting of planning, coordination, orders, reports, static intelligence, dynamic intelligence, and targeting information; and
- Administrative/sustainment – consisting of personnel and unit information, status reports, and sustaining information.

5-5. The commander, USSTRATCOM uses network operations (NETOPS) to direct the operations and defense of the DODIN. The DODIN is globally interconnected, end-to-end set of information capabilities, and associated processes for collecting, processing, storing, disseminating, and managing information on-

demand to warfighters, policy makers, and support personnel, including owned and leased communications and computing systems and services, software (including applications), data, and security. Refer to JP 3-12, *Cyberspace Operations* and FM 3-12, *Cyberspace and Electronic Warfare Operations* for additional information on cyberspace operations. NETOPS, in accordance with JP 6-0, *Joint Communications Systems*, provides integrated network visibility and end-to-end management of networks, global applications, and services across the DODIN, establishing maintaining, and protecting the DODIN. JFCC-IMD is the coordinating authority responsible for the planning of NETOPS and network defense for the BMDS. JFCC-IMD executes the planning, coordination, configuration control and operational oversight of BMDS communications on behalf of USSTRATCOM. Refer to ATP 6-02.71, *Techniques for Department of Defense Information Network* Operations for more information on the DODIN.

5-6. The main communication network used to support GMD is the ballistic missile defense communications network. GMD is supported by the communications architecture which connects strategic and regional missile defense. The ballistic missile defense network is comprised of numerous distinct communications systems including military and commercial satellite communications (SATCOM) and Defense Information System Agency provisioned terrestrial services. The BMDS communications architecture includes the GMD communications network and ballistic missile defense communications network. The ballistic missile defense communications network supports operations, research, development, test, and evaluation activities.

5-7. The ballistic missile defense communications network is a collection of telecommunications switching, routing, ancillary equipment, and interconnecting virtual circuits. It distributes BMDS information among subsystems, using the DODIN. The ballistic missile defense communications network provides communications links between the C2BMC suites, Aegis BMD, AN/TPY-2 (FBM), SBIRS, and the GMD fire control. The ballistic missile defense communications network includes all the data, voice, video, and transport systems independently installed and operated across multiple AORs supporting GMD. Additionally, they assist global and theater service providers with isolation activities, ensuring network outages affecting the BMDS are resolved in a timely manner.

5-8. The GMD communications network is a dedicated missile defense network providing communications connectivity for GMD components, such as sensors and weapons, to the GMD fire control nodes. The GMD communications network connects the components of GMD with a secure, fire control system for simultaneous missile intercepts. The GMD communications network integrates multiple separate sub-components collectively, capable of secure data, secure voice links, and encrypted long-haul multimedia communications links. It uses both government and leased civilian equipment. The fundamental criterion to select the components of the GMD communications network was the need to configure accurate and rapid voice and data networks.

5-9. The mission of the GMD communications network is to ensure commanders have access to the information required to execute the GMD mission. The network provides the infrastructure used to connect all missile defense assets, including sensors, weapons, and fire control nodes. The network includes the leased GMD communications network, commercial and military SATCOM, radio frequency line-of-site systems, tactical data link – joint, and all physical and logical links providing data and voice communications.

5-10. The GMD communications network is composed of long-haul communications, long-haul communications system manager, communications node equipment, and network system manager. The long-haul communications provides secure, reliable, multi-path, wide area network services between all geographically separated GMD locations, using fiber optic cable and SATCOM. The long-haul communications system monitors the health and status and controls the wide area network.

5-11. The communications node equipment and the network status monitor provide each GMD component access to the secure, survivable GMD wide area network. The communications node equipment is the portion of the GMD communications network subcomponent used to provide communications interface to each GMD component. Ground stations provide the data communications access to the GMD components within each local geographical area.

5-12. The network status monitor collection station, collocated with each communications node equipment, provides local communications and ground stations equipment performance monitoring, fault detection, isolation and resolution, and status reporting. Two network status monitor work stations are collocated with

each GMD fire control node. The network status monitor workstations are responsible for fault detection, insertion, recovery, and the issuance and tracking of trouble tickets, as well as ground stations system status reporting. Also collocated with each GMD fire control node is a maintenance execution center to facilitate coordination between the on-site sustainment centers and the system operators.

5-13. The GMD communications network is monitored and managed by the GMD communications network operations center. The GMD communications network operations center provides mission command, situational awareness, network security, safety, and network management roles and responsibilities for the GMD communications network. The GMD communications network includes all terminal site long-haul and local area network equipment to include encryption devices. It employs the commercial standards for telecommunications management network which includes the functions of fault configuration, accounting (asset management), performance, and security.

5-14. The GMD communications network operations center provides status reporting to the JFCC-IMD global IMD NETOPS integration center for distribution to appropriate combatant commands and the ballistic missile defense communications network. The GMD communications network operations center is responsible for network restoration, coordination of scheduled maintenance events, near real-time analysis of circuit performance, issuing of trouble reports, and resolving network status alarms. The GMD communications network operations center also implements transitions for simultaneous test and operations across the GMD communications network. These transitions are directed and implemented by the GMD communications network operations center network operators, engineers and trained and certified field engineers located at the various GMD terminal sites.

5-15. USNORTHCOM uses situational awareness data provided by the C2BMC system, GMD fire control remote workstation, and voice communication with the MDE of the 100th MD BDE (GMD) to exercise OPCON of GMD components. USSTRATCOM has OPCON of some GMD-related sensors. GMD fire control has the ability to directly task certain USSTRATCOM sensors in support of missile defense operations. Other sensors' support is coordinated through the C2BMC.

EXTERNAL SENSORS

5-16. Due to the various natures of the external sensor assets, the communications pathways differ. Space-based assets require ground station relay, sea-based assets use SATCOM and land-based assets use both fiber optic cable and SATCOM depending upon their location.

5-17. SBIRS satellites send data to the SBIRS mission control station. The mission control station currently disseminates information directly to both the C2BMC and GMD fire control.

5-18. The AN/TPY-2 (FBM) provides data to the GMD fire control system through fiber optic and SATCOM communications to the C2BMC system and then into the GMD communications network. The AN/TPY-2 (FBM) interfaces with the C2BMC network through the C2BMC network interface processor. Data is passed to the GMD fire control from C2BMC at the GMD fire control location. Execution of the sensor management function is through the C2BMC terminals, which are generally located remotely from the radar.

5-19. The UEWRs and COBRA Dane disseminate their data to the GMD fire control using a mixture of fiber optic cable and SATCOM depending upon their location.

5-20. The Aegis BMD uses Satellite tactical data link – joint and multicast tactical data link – joint to send data to the GMD fire control using the external system interfaces. These GMD components and sensors connect to the GMD fire control at the FDC and MDE via the GMD communications network and Defense Information Systems Agency provided long-haul communications. The GMD fire control nodes are connected to the C2BMC system used by USNORTHCOM via the GMD communications network with long-haul communications and the ballistic missile defense communications network.

5-21. The SBX provides its data to the GMD fire control using SATCOM into Earth terminals which relay information via fiber optic cable. The SBX operators have the ability to communicate directly with the GMD fire control operators using the ship-to-shore voice network and Secret Internet Protocol Router chat.

IN-FLIGHT INTERCEPTOR COMMUNICATIONS SYSTEM

5-22. The IFICS is a dedicated communications system for GMD fire control. It consists of a high-powered communication terminal and antenna designed to communicate with in-flight EKVs. IFICS establishes and supports nuclear-survivable data communication links between the IFICS data terminals and in-flight EKVs. The IFICS data terminals provide communication support for the transmission of in-flight target updates from the GMD fire control to the EKV and the reception of the in-flight status report from the EKV to the GMD fire control. Since the EKVs travel long distances, the IFICS must be located in diverse sites over a broad area to ensure line-of-sight with the EKVs at all times.

COMMAND AND CONTROL BATTLE MANAGEMENT AND COMMUNICATIONS

5-23. Through its communication architecture, C2BMC links ground and space-based sensors to display track and ballistic missile threat data which is distributed to each C2BMC suite. The C2BMC system consists of the battle management interface, the battle management subcomponents of each supporting weapon system, and the communications infrastructure for linking assets with other DOD and non-DOD networks. Sensor managers use C2BMC to control the AN/TPY-2 (FBM) radar.

RESPONSIBILITIES

5-24. The GMD communications infrastructure needs interoperable systems to facilitate the conduct of GMD operations against the threat. The organizations with responsibilities in GMD communications are uniquely organized to accomplish the GMD mission. Responsibility for providing communications resides with all agencies from the combat developer down to the Army GMD elements. The MDA is the developer, USSTRATCOM has the responsibility for GMD communication and JFCC-IMD is the asset manager for the ballistic missile defense communications network.

UNITED STATES STRATEGIC COMMAND

5-25. USSTRATCOM has responsibility for strategic communication for GBMD as defined within the USSTRATCOM Strategic Instructions. USSTRATCOM will leverage overall DOD communications architectures to support the Army GBMD forces by working with the joint force commander, Defense Information Systems Agency, combatant commands, and Services.

5-26. The BMDS leverages networks to provide connectivity for BMDS elements assuring commanders have access to information and data required to execute the BMDS mission. These existing NETOPS interoperate to form a virtual community of interest network, referred to as the ballistic missile defense communications network. The ballistic missile defense communications network includes data, voice, video, and transport systems independently installed and operated across multiple theaters supporting GBMD. The BMDS communications architecture is not a dedicated network for GBMD; rather, it shares the same transport and communications systems used to support multiple missions.

5-27. Its current infrastructure consists of both commercial and DOD satellites. Information system elements of BMDS, and various fragmented developmental and test networks connect to the ballistic missile defense communications network. The ballistic missile defense communications network includes operational, development, test, and training components of the Defense Information Systems Network, both hardened and non-hardened commercial and military SATCOM assets, Defense Red Switch Network, and the dedicated GMD communications network.

JOINT FUNCTIONAL COMPONENT COMMAND-INTEGRATED MISSILE DEFENSE

5-28. JFCC-IMD is the only asset manager for the mission communications portion of the ballistic missile defense communications network in support of the defense of the homeland. The combatant commands are responsible for asset management for theater and regional communications. JFCC-IMD is the primary responsible agency for the Tier I ballistic missile defense communications network. JFCC-IMD manages the ballistic missile defense communications network through the global IMD NETOPS integration center. The

global IMD NETOPS integration center is JFCC-IMDs continuous 24-hour global operations center responsible for monitoring and reporting availability, reliability, and security of the ballistic missile defense communications network and components directly supporting the ballistic missile defense mission. Additionally, they assist global and theater NETOPS service providers with isolation activities, ensuring network outages affecting the BMDS are resolved in a timely manner.

5-29. The ballistic missile defense communications network goal is to ensure all commanders have access to the information and data required to execute the GBMD mission and provide the infrastructure to connect all sensors, weapons, and battle management assets in IMD Tier I and Tier II nodes.

This page intentionally left blank.

Chapter 6

Security Operations

This chapter describes the security operations and procedures for the GMD specific and supporting sites. It also describes the threats to GMD, such as the proliferation of ballistic missiles, the threat of limited ballistic missile attack and the threats from physical attack and cyberspace to the missile site by protesters, terrorists, and subversives, along with the potential of irregular threats posed by opponents employing unconventional means to counter traditional United States advantages.

PROTECTION OPERATIONS

6-1. GMD installations face similar security environments as other high-priority defense installations. Complexity and geographic separation of the GMD components require thorough planning against threats, such as ground and air attacks, sea-based attacks on island or coastline facilities, and electronic and cyber-attacks. GMD components must also be vigilant against acts of terrorism, sabotage, and interference from protesters and agitators.

GROUND-BASED MIDCOURSE DEFENSE SECURITY

6-2. Preserving GMD capability includes protecting combatants and noncombatants personnel, physical security system level (SSL) assets, and information of the United States military. The protection warfighting function facilitates the commander's ability to maintain the force's integrity and combat power. Protection reduces the degree to which potential threats may disrupt operations. Emphasis on protection increases during preparation for missile engagements and continues throughout execution. Protection is a continuous activity and integrates all protection capabilities to safeguard GMD assets and protect forces. The protection warfighting function includes the following primary tasks:

- Coordinate air and missile defense support;
- Conduct personnel recovery;
- Apply antiterrorism measures;
- Conduct survivability operations;
- Conduct chemical, biological, radiological, and nuclear operations;
- Implement operations security;
- Implement physical security measures;
- Conduct police operations;
- Provide force health protection;
- Provide explosive ordnance disposal;
- Conduct detention operations;
- Conduct populace and resource control;
- Conduct area security;
- Perform cyberspace security and defense;
- Conduct electromagnetic protection; and
- Conduct risk management.

6-3. Continuous intelligence gathering and analysis is critical to effective security of GMD system resources. Commanders working with their DOD and Service component intelligence agencies, and USSTRATCOM special security and counterintelligence, must analyze potential threats. Intelligence analysis shall consider current local, regional, and international factors bearing on the security threat to

installations and GMD system resources. It stresses the known capabilities of hostile elements to damage, destroy, or impede the planned use of SSL resources. Commanders will use USSTRATCOM postulated threats to GMD systems and any theater specific threat assessments to develop local threat assessments. Commanders shall conduct formal risk and vulnerability assessments of the GMD system resources in their custody. Up-to-date threat assessments shall be developed and maintained as a vital part of evaluating the overall security of GMD system resources.

SECURITY AND DEFENSE

6-4. It is the commanders' responsibility to apply the more stringent security standards required by USSTRATCOM Strategic Instructions, the Army, and BMDS security during increased threat levels or high risk determinations, or as the commander and director deems necessary. The objective of security for the GMD sites is to:

- Implement general policy for the security of personnel, installations, military operations, and designated assets in accordance with USSTRATCOM Strategic Instructions, DOD 5200.08-R and Army applicable security regulations;
- Provide security guidance and general procedures which are realistic, harmonized with other security disciplines, and provide the necessary flexibility for commanders to protect personnel, installations, projects, operations, and related resources against capable threats from terrorists, criminal activity, and other subversive or illegal activity;
- Reduce the loss, theft, diversion of, or damage to DOD assets with advanced technologies; thereby enhancing overall security, while ensuring warfighting capability is maintained;
- Standardize personal identification and authentication to DOD installations and facilities, including interoperability with other Federal entities; and
- Utilize the DOD personal identity verification credentials on the Common Access Card as the universal authority of individual authenticity.

6-5. GMD assets are possible targets for sabotage. It is essential frequent and periodic security assessments are made of the potential threat and the risks and vulnerabilities associated with the GMD security program. Other considerations are:

- The postulated threat to GMD assets, defended areas, and USASMDC annual threat statements, local threat, and all other relevant factors will be considered;
- Security programs will be revised accordingly to ensure adequate protection at all times;
- Physical security processes must constitute a balanced, in-depth system responsive to all credible and potential threats and vulnerabilities; and
- Construction projects require continuous security coordination between engineers and security personnel from planning through completion of the project.

DAY-TO-DAY OPERATIONS

6-6. During day-to-day operations for the GMD sites, all posts at the site are staffed. However, security forces must be prepared to react and negate a threat according to pre-established plans and rules for use of force. The importance of training to react in a crisis cannot be overemphasized. Not all scenarios will allow for a smooth progression. For example, a no-notice attack or penetration attempt could cause immediate transition to crisis operations, thus highlighting the significance of intelligence, extensive preplanning, and personnel and asset management.

Designated Response Force

6-7. A unit designated by the commander to respond to threat attacks or emergency situations. The designated response force is typically task-organized for the specific threat or incident in which it is tasked to respond, and may include military police, firefighters, chemical, biological, radiological, and nuclear personnel, and medical personnel.

6-8. Within GMD sites, the designated response force is required for a show of force to repel and control civilian protestors and defeat or delay any attacking force. In the current force design, for normal operations,

the military police security platoon inside the missile defense complex provides sufficient military police in multiple teams to respond to intrusion alerts. Teams are deployed in specified areas and one team serves as a designated response force to support the other four. All teams are mounted and armed in accordance with military police doctrine and local standard operating procedures. Reaction and response times must be determined through exercises and drills while taking into consideration the layout of the missile defense complex and missile operational safety requirements recorded in unit standard operating procedures.

Reserve Force

6-9. Army doctrine outlines the designation of a reserve force. A reserve force is an uncommitted force available for action at the decisive moment. Its primary purpose is to retain freedom of action throughout a contingency operation. The designated reserve force consists of the members of the platoon (-) on mission cycle inside the wire, who are not staffing a post or otherwise engaging the threat. Once the designated response force and the remainder of the platoon (-) is committed, the commander immediately reconstitutes a reserve force from the company (-) to retain freedom of action.

PHYSICAL SECURITY PROGRAM

6-10. Physical security is a primary command responsibility and is the responsibility of commanders, directors, supervisors, and officers in charge, whether military or civilian. The physical security program is part of security concerned with active and passive measures designed to prevent unauthorized access to personnel, equipment, installations, information, and to safeguard them against espionage, sabotage, terrorism, damage, and criminal activity. In accordance with AR 190-13, physical security programs will provide the means to counter GMD threat entities during peacetime, mobilization, and wartime. These include:

- Hostile intelligence services;
- Foreign military and paramilitary forces;
- Terrorist or saboteurs;
- Criminal elements;
- Protest groups; and
- Insider threats.

Note. See ATP 3-39.32, *Physical Security* for more information on the physical security programs.

CYBERSECURITY

6-11. The MDA operates a robust program protection plan to counter threats to all aspects of the GMD program. Emerging threats, vulnerabilities and susceptibilities will be evaluated against current countermeasures to determine whether countermeasures already in place are adequate for emerging items or whether new countermeasures should be considered and fielded.

SECURITY SYSTEM LEVELS

6-12. In accordance with USSTRATCOM Strategic Instructions, SSLs are identified for specific GMD assets which must be properly secured, and the security resources dedicated to those assets. SSL-A resources assigned to GMD units are resources for which the loss, theft, destruction, or misuse would result in great harm to the strategic missile defense capability of the United States. The SSL-A security level must result in the greatest practical deterrence against and response to hostile acts. In-place security measures should provide an effective means to achieve detection, interception, and defeat of a hostile force before it is able to seize, damage, or destroy resources. Entry control for SSL-A and –B restricted areas is conducted by posted entry controllers through a single entry point whenever practical.

6-13. All equipment and resources required to be operational to perform this mission are considered. The SSL-A resources physical security system consists of redundant integrated, layered, multi-technology

subsystems for intrusion and detection coverage during all site-specific weather conditions. SSL-A security resource planning for physical security systems should consider the use of the following:

- Entry control facility (ECF). The ECF is located at the boundary fence and allows personnel and vehicle inspection prior to entering the site. All personnel pass through the personnel entrapment area where they are required to present valid credentials to gain access to the restricted area.
- Vehicle crash barrier;
- Vehicle entrapment area;
- Security control center which houses the integrated electronic security system control room and communications equipment to support mission command;
- Perimeter security fence line is a physical access barrier to the restricted area which consists of two concentric fences separated by at least 30 feet and has lighting on all sections;
- Video and infrared cameras with full view of perimeter security fence line; and
- Defensive fighting positions which provide 360 degrees of protection for security.

SECURITY FORCES AND USE OF FORCE

6-14. There will be sufficient security forces assigned and designated to provide necessary security requirements. Security forces will be organized, trained, armed and equipped to provide normal day-to-day protection for GMD assets and to react to security incidents. The location and types of facilities to be secured will drive the type of security provided.

6-15. Delay must be long enough to allow security forces to respond to and neutralize the threat before they gain access to the protected facilities containing GMD assets. Assessing the adequacy of the security of GMD assets will be an essential task for the responsible commander. The postulated threat to GMD assets, including intelligence on local threats and other relevant factors will be considered. Security programs and procedures will be revised accordingly to ensure adequate protection. Threat analyses or other security considerations may lead to doubt adequate protection is provided from available resources.

ENTRY CONTROL OPERATIONS

6-16. Day-to-day operation for entry to the site is a multilevel operation. Arranging authorization to the site is through the Joint Program Office, unit intelligence staff section, and site security personnel. Authorizing the prime contractor access to the site requires security forces to have a continuously updated list of authorized personnel, and coded to reflect precisely which facilities each individual is working. Guard personnel perform entry control of vehicles, inspection, and clearing by proper authorities and controls before reaching the GMD site (see AR 190-13 and ATP 3-39.30). For example, prime contractor technician must have access to the power generation facilities, but has no reason to enter either the readiness and control building or the missile field. Therefore, when the individual provides proper identification at the entry control facility, access will be granted only to the areas the individual is authorized, such as the power generation facilities. This method of control does not allow access to other facilities or areas.

Installation Entry Control Facility Security Forces

6-17. Each installation ECF is staffed by armed security force personnel (Soldiers, Department of Army civilian police, security guards, or contract guards) as permitted by applicable federal, state, and territorial statutes, and status-of-forces agreement or host nation agreement. Procedures will be established for each installation ECF, and will be reviewed at least annually and revised, as necessary. Commanders outside the continental United States may continue to use current forms of identification, and continue background checks to allow installation access to foreign nationals, contractors, and vendors per status-of- forces agreement and other theater regulations.

6-18. Commanders will use headquarters, Department of the Army (DAPM–MPP–PS) cybersecurity staffing guidance for manpower considerations to determine the appropriate manpower for installation ECFs. Security forces will be provided with:

- Adequate means of communications;
- Appropriate weapons and ammunition and trained in their care and use per AR 190–14; and

- Personal protective equipment.
- Training and weapons qualification of security force personnel will be in accordance with applicable directives, AR 190-56 for all assigned Department of the Army civilian police and guards, and the statement of work for contract security guards. Training will also include:
- Recognition of sabotage-related devices and equipment which may be used against the installation;
- Use of devices to identify sabotage-related devices and equipment, such as hand-held vapor tracers and vehicle and cargo inspection systems; and
- Authorized forms of identification for access to the installation.

Visitor Escorts

6-19. Occasionally, it is necessary to escort personnel who do not have the minimum security clearance required to be granted access to a GMD facility. Approved personnel shall escort cleared visitors within all controlled areas. All GMD units shall have established policies and procedures for escorting visitors.

Communications

6-20. The security force is equipped with two-way radios, which are essential for the efficient operation of the security force and the accomplishment of its assigned mission. The integrated electronic security system alarms and sensors operator maintains the security force net. All on-duty security force personnel have an individual radio, and the security force vehicles have vehicle-mounted radios. The installation or garrison security force has compatible communications equipment to allow continuous coordination between the two organizations when the mission dictates. Secure voice capabilities are used when possible.

WEAPONS

6-21. Weapons will provide the maximum practical firepower for security forces, whether carried or immediately available. Where employing side arms, personnel responsible for force protection condition of SSL resources will have immediate access to weapons providing greater firepower. Security forces shall be equipped and armed for combat operations and terrorist incidents as determined appropriate by the local commander. The local environment must be considered in authorizing the types of weapons employed.

6-22. Because of the high number of civilian personnel onsite, the military police commander will brief the military police force on the rules for the use of force before receiving weapons. Issuing of weapons to military police personnel will be in accordance with AR 190-14 and the unit standard operating procedure. The commander may prescribe other weapons to the security force based on needs and requirements. Normally, weapons are loaded with live ammunition, except when prohibited for safety reasons. Criteria is established to authorize lock and load procedure in prohibited areas. The use of privately owned weapons while on duty is not authorized. Weapons and ammunition issued to security-force personnel are not removed from the installation, except for official duty.

AMMUNITION SUPPLIES

6-23. Ammunition supplies maintained for security force use are on the GMD site in secured storage containers, according to AR 190-11. According to the intelligence picture and the reinforcing support available, a basic load of ammunition is kept on hand sufficient to support site defense against a full level II threat for an extended duration.

SECURITY PLANNING FACTORS

6-24. The following security planning factors must always be considered:

- GMD system components (GMD fire control, LMS, and GBIs) are designated a SSL-A asset, as defined by USSTRATCOM Strategic Instructions;
- ARNG AGR personnel staff the military police GBI security company;

- The equipment designated in the table of organization and equipment and table of distribution and allowance must be available; and
- GMD GBI sites and other selected local GMD assets are designated as restricted areas.

THREAT DESIGN

6-25. Changes to the threat guidance have occurred since the approval of the initial GMD unit structure in July 2001. The security force design may undergo other changes as GMD systems evolve. The security force leaders may need to manage operations aggressively to continue to succeed with the available forces. This appendix provides a framework from which to base future adaptations.

6-26. The threat to, or aggressors against GMD systems may be criminals, vandals, activists, extremists, protest groups, terrorists, or enemy forces. They may employ all possible tactics to include, moving vehicle bombs, stationary vehicle bombs, small arms and standoff attacks on the facility, forced or covert entry, insider compromise, visual, acoustic, and electronic-emanations surveillance, mail and supply-bombs, airborne and waterborne contamination, and intrusion or attack to achieve their intended purpose. Determine the tactics the aggressors use, such as vandalism, public attention, disruption, or destruction of GMD systems.

6-27. Threat assessment is continuous. The GMD unit commander, installation commander, and the security force continuously review and assess threats to the GMD installation. Normally, threat assessment is an intelligence staff responsibility. The intelligence staff focuses on the threat, to include regular, irregular, and hybrid threats. Within the United States, the Federal Bureau of Investigation has primary responsibility for both foreign and domestic terrorists, and the United States Army Criminal Investigations Command has criminal intelligence collection capability.

6-28. Military police conduct police intelligence operations to support the operations process and protection supporting tasks by providing police information and police intelligence to enhance situational understanding, protect the force, enable the rule of law, and assist homeland security. Military police collection assets collect and process police information during military police operations concerning crime, disorder, criminal activity, and criminal threats. Collected information focuses on the aspects of the operational environment that cause or influence crime, disorder, and fear of crime within a population. Military police leaders, staffs, and police intelligence analysts produce police intelligence through analysis and the integration of criminal intelligence (strategic and tactical) and crime analysis (administrative, strategic, and tactical) about crime, disorder, criminal activity, and criminal threats throughout the operational environment.

6-29. The force design of the military police GBI security company organization is to defeat up to a level II threat and delay a level III threat. Military police GBI security company forces employ organic platoons, standard procedures and tactics, and external assistance arrangements to resist attacks by small tactical units and enemy special operations forces. The security company accomplishes security coordination in accordance with unit standard operating procedure and memorandum of agreement with the garrison security forces and local and state law enforcement. : Refer to FM 3-39 for additional information on Military Police operations.

FORT GREELY SECURITY

6-30. GMD operations and related site security at Fort Greely are federal military missions. ARNG and AGR Soldiers performing the site security portion of the GMD mission transition from a Title 32 to Title 10 Federal status in accordance with the Secretary of the Army approved staffing model. When performing the site security for the GMD mission, ARNG and AGR Soldiers are in a Title 10 federal status under the command of the 49th MD BN (GMD). Security for GMD resources in Colorado is the responsibility of and provided by security forces at Schriever Air Force base. USASMDC security-related GMD responsibilities include:

- Title 10 command of Soldiers performing security for the GMD mission;
- Organize, train, equip, and supply Army forces to maintain and operate the site security system;
- Design and direct an evaluation and certification program for Army security crews to achieve specified standards;

- Managing USASMDC support responsibilities; and
- Coordinate with Joint Program Office, Army Service component command, combatant commander, and the state ARNG to ensure support of the installation commander for the site security mission.

6-31. The 49th MD BN (GMD) commander directly supports the 100th MD BDE (GMD), USASMDC, and the Joint Program Office by providing physical security for the site and other selected GMD assets. The commander's responsibilities include:

- Command over Soldiers performing GMD mission;
- Plan and conduct day-to-day GMD operations, such as training, exercises, and maintenance;
- Support security system readiness evaluations and certification program for Army security crews to specified standards;
- Conduct real-time operational and tactical planning for potential attacks and site penetration attempts;
- Provide physical security recommendations to Joint Program Office, USASMDC, and 100th MD BDE (GMD) to improve site physical security preparation in response to espionage, sabotage, terrorism, and damage; and
- Conduct the tactical execution of the security mission and provide performance assessment of Soldiers performing the GMD mission.

6-32. USASMDC establishes policies governing GMD site security and the 49th MD BN (GMD) commander has overall responsibility for GMD site security. The GMD site installation commander has overall responsibility for physical security and protection of the installation, and establishes installation policies for personnel protection and physical security measures.

GROUND BASED INTERCEPTOR SITE SECURITY OPERATIONS

6-33. The military police GBI security company is responsible to conduct critical site security on the missile defense complex in order to secure and defend GMD resources. This security is for worldwide GMD operations. The GBI security company provides tactical forces to detect, identify, and eliminate hostile threats to the missile defense complex. In accordance with USSTRATCOM Strategic Instructions, specified resources on the missile defense complex are provided protection as a designated SSL-A resource. Unit capabilities are; fixed facility security for a GBI site, designated response force personnel, physical security survey and inspection, defense of the GBI area, planning, direction, and coordination of the physical security activities on site, and defend the site facility. The task organization for security operations for any future site will have to be developed based upon the specific postulated threat, distances security forces must travel, environmental considerations, configuration of the site, and the number of SSL-A resources.

6-34. The organization of the security company has a headquarters section and three military police security platoons. The military police GBI security company commander is the principal security advisor for the 49th MD BN (GMD) commander and staff. Each platoon is task organized to provide:

- Security of the FDC and missile sites;
- ECF with staffing to support an integrated electronic security system;
- Designated response force;
- Sergeant of the guard;
- Roving patrols for each duty cycle; and
- Personnel security oversight of the contractors and Soldiers working within the GBI missile fields.

6-35. The military police platoons are organic to the military police GBI security company and provides physical security to the GMD GBI site. Each platoon is equipped with the appropriate weapons, night vision devices, and radios in common with military police companies. The platoon is composed of a platoon leader, platoon sergeant, and four squads.

6-36. The military police Platoon Leaders are responsible to the company commander for the platoon combat readiness, training, discipline, and maintenance of platoon equipment. The platoon leaders direct the execution of the platoon missions, based on the company commander's priorities. The platoon leaders are

responsible for ensuring the physical security and protection of the warfighting function according to the commander's intent. The platoon leaders function as the officer of the guard for the GBI site.

6-37. The platoon sergeants lead elements of the platoon, as directed by the platoon leaders, and assume platoon command in the absence of their platoon leaders. The platoon sergeants direct the platoon day-to-day activities ensuring all required individual and team training and sustainment needs are met. During physical security and protection operations, the platoon sergeants may assist in the control of the platoon. When on shift, the platoon sergeants function as the sergeant of the guard for the GBI site.

6-38. The military police squads each have the manpower to staff three shifts for continuous 24-hour operations. The military police squads are task organized to provide staffing for entry control, electronic security system monitoring, SSL-A response forces, and a security control center.

- ECFs are designed to assist security forces in controlling entry and exit from restricted areas. The ECF requires security personnel on duty at all times in order to perform the required tasks of badge exchange, personnel search and vehicle search. All personnel and vehicles entering and exiting the missile defense complex pass through the ECF with the personnel searches and issuing of badges in one part of the building, and vehicle searches conducted in a separate part of the building.
- Electronic security system monitoring is the responsibility of the sergeant of the guard. From this location, the sergeant of the guard directs the monitoring of the integrated electronic security system and directs the activities of the designated response forces. One individual is required to operate the integrated electronic security system alarms and sensors, which consists of perimeter cameras and other sensors. The number of cameras depends upon the size, construction, topography, and climate for the missile defense complex.
- Security response team or designated response force will have a dedicated security response team posted for each SSL-A resource. Additionally, a designated response force will be posted for the entire missile defense complex as supporting forces for the other response teams. Security force personnel shall not be tasked to perform functions unrelated to the security mission while on duty.
- Security control center is required at every installation supporting SSL-A, -B, or –C resources to provide command, control, and communications for on-duty security forces. From this location, Soldiers direct the monitoring of the integrated electronic security system and the activities of the designated response forces.

AUTHORITY AND JURISDICTION

6-39. The commander of the 49th MD BN (GMD) and the installation commander determine the extent and limitations of the site security force's authority and jurisdiction. Jurisdiction on Fort Greely is a complex issue; other GMD site locations may have similar issues to resolve. The servicing legal office or provost marshal will answer all issues relating to jurisdictional questions.

6-40. Areas outside the site are subject to Federal, state and local authority, depending on the actual location, law enforcement agreements, and specific law enforcement personnel. The local Office of the Staff Judge Advocate or provost marshal will provide information and advice in regard to federal, state and local authority.

6-41. Security procedures will be developed and implemented for any and all future GMD facilities as they become operational. Security procedures for the globally dispersed sites are unique to each location and will continue to be so as additional assets are activated.

ADDITIONAL LOCATIONS

6-42. GMD sites and supporting element sites are globally distributed and face unique security concerns. Each location has its own security procedures established to counter the foreseen threats.

6-43. Security for Detachment 1, 100th MD BDE (GMD) resources are the responsibility of and provided by security forces at Vandenberg Air Force Base. This site differs from Fort Greely by environmental conditions and the wide spread distribution of GMD assets on the installation.

6-44. The Fort Drum security detachment is staffed by Department of the Army civilians under the supervision of military personnel. They provide security for the GMD assets located on Fort Drum.

GENERAL THREATS TO GROUND-BASED MIDCOURSE DEFENSE RESOURCES

6-45. The threats from ballistic missile attacks are numerous and they continue to expand. Expanded technology and proliferation of strategic ballistic missile capabilities expand the complexity of protecting the United States homeland and friendly forces. The proliferation of weapons of mass destruction, coupled with a conventional means of delivery greatly increases potential lethality of any adversary and elevates the importance of employing a robust BMDS capability to protect United States homeland, deployed forces, friends, and allies.

6-46. The detection capabilities, engagement ranges, mobility, and lethality of launch sites have significantly increased. Ballistic missiles are instruments of political coercion. Political targets include civilian population centers and government, cultural, and religious structures and locations. Additionally, propaganda value exists in attacking United States and multinational forces to show their vulnerability, particularly in European countries.

6-47. Attacks may likely be against a variety of targets, such as GMD sites, contributing sensor elements, communications nodes, and key civilian facilities like population centers.

> *"The contemporary and emerging missile threat from hostile states is fundamentally different from that of the Cold War and requires a different approach to deterrence and new tools for defense. The strategic logic of the past may not apply to these new threats, and we cannot be wholly dependent on our capability to deter them. Compared to the former Soviet Union, their leaderships often are more risk prone. These leaders also see weapons of mass destruction as weapons of choice and not of last resort. Weapons of mass destruction are their most lethal means to compensate for our conventional strength and to allow them to pursue their objectives through force, coercion, and intimidation. The probability that a missile with a weapon of mass destruction will be used against United States forces or interests is higher today than during most of the Cold War, and it will continue to grow as the capabilities of potential adversaries mature."*
>
> National Security Presidential Directive 23

6-48. The missile threat to the United States, allies, and forward-deployed forces include all ranges of ballistic missiles and submarine launched ballistic missiles. Although technologically far more difficult to develop and deploy, submarine launched ballistic missiles are a challenge to defend against because once a ballistic missile submarine is submerged at sea, the ability to predict and prevent a submarine launched ballistic missile strike becomes inherently much more difficult.

6-49. Ballistic missile attacks are envisioned in three potential limited attack scenarios:

- Authorized attack — Leadership of a nation-state, multinational forces, or non-state actors (including terrorists) may authorize a premeditated launch against the United States;
- Unauthorized attack — Insurgent groups or other radical elements may perpetrate a premeditated attack against the United States by a nation-state, multinational force, or group, but is not accidental; and
- Accidental launch — Unintended launches may result from a random event, such as mechanical failure or human error, which threatens the United States.

6-50. The global threat environment presents four types of complex, interrelated, persistent, and emerging security challenges – traditional, irregular, catastrophic, and disruptive. Many of these threats include non-state actors not deterred by our military superiority, and in fact, are motivated by our superiority.

6-51. The persistent and emerging challenges for Army GMD assets include many of the issues in the homeland security environment. However, the boundaries are neither precise nor discrete and in most situations will overlap geographic combatant commander AORs, occur simultaneously, or offer no easily discernible transition from one challenge to another challenge.

- Traditional challenges. Traditional threats of aggression from regional adversaries or an adversarial multinational force remain the most dangerous, demanding, and intensive missions for military forces. States will continue to resort to strategies based on the use of military power to achieve their goals, in conflicts covering the range of military operations, and occur in unforeseen locations and conditions.
- Irregular challenges. The immediate threat the United States faces is the irregular challenge. General characteristics of irregular warfare include protracted struggle, reliance on sanctuaries and outside support, gradual escalation in number and size of tactical actions, and the predominance of close combat as the means of engagement.

6-52. Adversaries will make extensive use of information operations to include electronic warfare, computer network operations, and the use of radiofrequency weapons in order to disrupt, delay, or degrade United States forces command and control systems and active defense measures.

6-53. Information Operations. The threats to the GMD information infrastructure are genuine, worldwide in origin, technically multifaceted, and growing. Today's threats come from individuals and groups motivated by military, political, social, cultural, ethnic, religious, or personal gain. Adversarial information efforts against GMD (see FM 3-13) are the employment of the core capabilities of electronic warfare, computer network operations, psychological operations, military deception, and operations security. These capabilities are used in concert with specified supporting and related capabilities to affect or defend information, information systems, and to influence decision making.

6-54. Protesters. Security forces consider violent protesters a threat. Protesters include the two general groups of vandals and extremist protesters. Both groups are politically motivated and act out of frustration, discontent, or anger against the actions of other social or political groups. The primary objective of both groups commonly includes destruction and publicity.

6-55. Asymmetric warfare. The threats:

- At the operational level, cyberspace attack on computer networks may disrupt the transfer of information.
- At the tactical level, enemy special operations forces or terrorists could attack GMD sites or nodes in the confusion resulting from cyberspace or weapons of mass destruction attacks.

6-56. A deliberate or unauthorized ballistic missile attack could precede (or accompany) a conventional attack on GMD systems. Threats to GMD installations include those associated with high priority defense. These threats may be ground, air, sea, and information operations attacks on facilities, or forms of terrorism and sabotage.

Chapter 7

Sustainment

This chapter describes the Army's duties and responsibilities for sustainment support of GMD. The MDA is under authority, direction, and control of the Under Secretary of Defense for Acquisition, Technology, and Logistics responsible for managing, directing and executing the development of the GMD. As such, it is an acquisition agent whose development activities make them responsible for planning, acquiring, and implementing activities necessary to support Army GMD elements. However, it is imperative support be responsive on a noninterference basis. This is critical given the importance of the GMD mission to defend the homeland, deployed forces, friends, and allies from ballistic missile attack. The sustainment concept for operations is complex and Army personnel should be familiar with its impact on readiness and availability.

OVERVIEW

7-1. The responsibility for GMD logistics support extends into a combatant command AOR and may be modified when logistic support is otherwise provided for by agreements with host nation agencies, Services, or by combatant commanders. The combatant command may determine common servicing would be beneficial within the AOR or a designated operational area. If so, the combatant command may delegate the responsibility for providing or coordinating service for all Service components in the AOR or designated area to a specific Service component. Service components will identify and validate support requirements in both the deliberate and crisis action planning processes, and then provide these requirements to the supporting Service component as soon as possible.

GROUND-BASED MIDCOURSE DEFENSE SITE CHARACTERISTICS

7-2. GMD has several characteristics which may affect its sustainment. These characteristics include:

- The GMD system is neither mobile nor deployable, therefore, permanently situated sites or sites which include large, fixed structures, are affected by local weather.
- Limited numbers of sites create a very low density of equipment items and trained personnel to maintain and operate equipment.
- Continuous 24-hour operations. Staffing is consistent and include careful scheduling of maintenance and training activities.
- GMD systems requires an extensive contractor support maintenance concept, which requires contractor life-cycle support. This is an outcome of the GMD systems being low density, highly complex, with a dual role as operational and test.
- Planned upgrades are in phased incremental capability deliveries. Successive capability deliveries increase the overall capability of the system to meet the evolving threat. However, these planned upgrades pose operational and sustainment challenges.

SUPPORT CONCEPT

7-3. Originally, GMD was a test bed operation primarily designed to serve as a test and development environment. In response to National Security Presidential Directive 23, the Secretary of Defense directed GMD provide an initial, limited defensive operational capability as soon as possible. However, the requirement to use GMD as a test bed to perform non-operational development, test, exercise, training, and maintenance activities remained. The requirement to allow concurrent or simultaneous use of the GMD system to conduct both tactical operations and other necessary activities remains in effect. Concurrent or

simultaneous means regardless of any non-operational activities taking place, a minimally defined set of resources is continuously available and on operational alert. Consequently, the support concept developed to meet the varying needs of this system are broad and cannot simply focus on operational support.

PRINCIPLES OF SUSTAINMENT

7-4. Successful support must be both effective and efficient. Sustainment operations are not successful unless they provide effective support. Support of the commander's plan is the goal of all sustainment efforts. Effective support requires a thorough understanding of the commander's intent and synchronizing support plans with the concept of operations. Efficiently planned sustainment operations ensure scares resources, such as personnel, time, equipment or material, are not wasted during sustainment operations. Effectiveness, however, must not be handicapped by efficiency. These two aspects of sustainment and logistics are balanced to provide the foundation of successful operations. Even though GMD is unique in many aspects, there are eight common Army characteristics of support which apply to facilitate effective and efficient support operations and enable success. In accordance with ADP 4-0, the eight principles are integration, anticipation, responsiveness, simplicity, economy, survivability, continuity, and improvisation.

- Integration is the incorporation of all principles of sustainment into operations to ensure mission success. This becomes even more imperative when conducting joint and multinational level operations.
- Anticipation is the ability to determine what is required ahead of time, and to provide the minimum essential supplies and services required to begin operations. The commander's logistic staff develops the concept of logistic support, completes the logistic estimate, and initiates resource identification based on the supported commander's requirements, priorities, and apportionment.
- Responsiveness is the right support in the right quantity in the right place at the right time. Among the logistic principles, responsiveness is the keystone; all else becomes irrelevant if the logistic system cannot support the concept of operations of the supported commander.
- Simplicity often fosters efficiency in the planning and execution of national and AOR logistic operations. Mission-type orders and standardized, interoperable procedures contribute to simplicity. Establishment of priorities and pre-allocation of supplies and services by the supported unit may simplify logistic sustainment.
- Economy is achieved when effective support is provided using the fewest resources at the least cost, and within acceptable levels of risk. At some level and to some degree, resources are always limited. When prioritizing and allocating resources, the commander must continuously consider economy and optimize use of resources to ensure effectiveness and mission success while supporting every effort toward achieving efficiency.
- Survivability is the capacity of the organization to prevail in the face of potential destruction. Logistic units and installations are also high-value targets which must be safeguarded by both active and passive measures. Active measures include a defense plan for supply with provisions for reinforcement and fire support. Passive measures include dispersion, physical protection of personnel and equipment, deception, and limiting the size of an installation to what is essential for the mission.
- Continuity is a measure of the ability to maintain logistic support to all users throughout the AOR for the duration of the operation. Continuity focuses the supporting commander's attention on long-term objectives and capabilities of the supported forces. Long-term support is a challenge for the logistician, who must not only attain the minimum essential materiel levels to maintain readiness and conduct operations, but must also sustain those operations.
- Improvisation is the ability to adapt logistic structures and procedures to changing situations, missions, and concepts of operation. Logistic plans and operations must be flexible in order to achieve both responsiveness and economy. This principle is a guide for strategic thinking and forms the template for synchronized and coordinated joint logistic planning.

GMD SUSTAINMENT CONCEPT

7-5. The government furnished equipment support concept provides support to the commander by including:

- A single life-cycle support contractor who is responsible for all system peculiar maintenance support and is responsive to the commander's direction. Through its prime contractor support system, the prime contractor will manage all logistical areas of maintenance and system upgrades;
- Supply support;
- Support equipment, training, and training devices;
- Technical data;
- Computer resources;
- Facilities and system facilities maintenance; and
- Packaging, handling, storing, and transporting.

7-6. Commanders must have a thorough understanding of the contractors' statements of work and their benchmarks and provisions for ensuring responsive and appropriate logistics support. The centralized logistics management support structure is under the support contractor's responsibility as detailed below.

- A logistics control center is the support contractor's responsibility. The logistics control center provides a single point of contact for all sustainment actions and readily accessible sustainment information, such as repair parts usage, due-ins, equipment status, and equipment readiness reporting data.
- The contractor operates the on-site control center tailored to the needs of the assets at each location.
- The on-site support center is the main element through which the contractor manages the maintenance support of elements and reports to the commander. Within the on-site support center, the maintenance management center is the single point of contact to facilitate the military oversight of the support contractor, and ensures the contractor's responsiveness to the commander's direction.
- The maintenance of government furnished equipment exists at two levels: on-site, unit-level maintenance and off-site, depot-level maintenance. Some depot-level maintenance may be performed onsite due to the requirement for continuous 24-hours operations.
- Extensive use of both diagnostic and prognostic maintenance capabilities using build-in test equipment, built-in test, and condition based maintenance plus procedures to automatically predict, detect, and isolate faults down to the line replaceable unit without interfering with mission performance while the system is operating.
- The contractor replaces the line replaceable unit and repairs it onsite or offsite, as required.
- For the long term, the Army considers the use of commercial equipment and practices best for the fixed sites.
- Reach back – While different from JP 3-30, BMDS transition transfer plan defines this as the use of GMD prime contractor assets outside of the support contract when it becomes necessary to sustain acquisition or construction, maintenance, operation, and disposition of facilities.
- Operators and maintainers determine system capability failure analysis criteria to evaluate system's capabilities, to determine if components will fail during crisis or combat operations.
- Logistics considers the parameters which have negative effects on the probability of engagement success, such as time to troubleshoot, time to repair, availability of line replaceable unit for repair operations, criticality of defended asset, and time to impact. These criteria determine if operations proceed or if a system is taken offline for repair.
- MDA will continue to have primary responsibility for execution of current and future development and production contracts, which encompass the hardware and software development efforts, obsolescence risk reduction, testing, and site system hardware procurement. They retain responsibility for software configuration management and for post deployment software support.

7-7. The key imperative is, contractor support must be responsive to the military commander and provided on a noninterference basis. This is critical given the importance of the GMD mission and the need to generate

forces in crises. Commanders must be familiar with ATP 4-10 to ensure contractor operations support the mission.

CONTRACTOR LOGISTICS SUPPORT

7-8. The maintenance strategy is a two-level maintenance concept referred to as field and sustainment maintenance per AR 750-1. The Army normally refers to this concept as organizational and depot levels of maintenance. However, since supporting the BMDS components are conducted via contractor logistics support, the field and sustainment maintenance is often referred to as on-site and off-site maintenance. The prime contractor is responsible for identifying and accomplishing on-site tasks, and tasks which require equipment to be sent off-site for repair or replacement by the prime contractor or the original equipment manufacturer.

7-9. On-site maintenance will consist of tasks performed on both the installed BMDS equipment and removing failed items for repair at maintenance facilities within the compound. All maintenance activities are through contractor life cycle support. The prime contractor is responsible for planning, acquiring, and implementing all activities necessary to support the program. In order to maintain a small foot print, some support equipment and services may be obtained from the host command or host nation.

7-10. Off-site maintenance will be performed by the prime contractor or the original equipment manufacturer as agreed upon between the Army and the material developer. Off-site maintenance includes depot level repairable items, other unit maintenance, such as environment and transportation, and initial spare parts as required.

7-11. Condition based maintenance plus, is the application and integration of appropriate processes, technologies, and knowledge-based capability to improve the reliability and maintenance effectiveness of DOD systems and components. Condition based maintenance plus, is maintenance performed on evidence of need provided by reliability centered maintenance analysis and other enabling processes and technologies, such as system health monitoring and management using embedded sensors. To the commander, condition based maintenance plus, is the ability to meet mission requirements with proactively driven maintenance, as well as the ability to optimize the competing demands of warfighting and planned maintenance.

PRIME CONTRACTOR SUPPORT SYSTEM

7-12. The deployment and maintenance system of the prime contractor provides contractor logistics support to meet the readiness objective for the fielded GMD elements. To accomplish this, the deployment and sustainment system has put in place a prime contractor support system which uses a two-level maintenance concept of on-site and off-site maintenance. The office of emergency management and the prime contractor develop and implement a single integrated support infrastructure as the method for implementing an executable support system.

7-13. The prime contractor support system is composed of organization, functions, information systems, tools, and a communications infrastructure. The deployment and maintenance system support organization centrally manages the prime contractor support system through the Huntsville monitoring center, located at the prime contractor facility.

7-14. Prime contractor support system overview:

- Prime contractor support system provides the support infrastructure and maintenance management system for support of GMD prime mission equipment, associated support equipment and operational facilities;
- Provides centralized management of the support system;
- Off-site support centers execute hands-on maintenance of prime mission equipment at sites;
- Off-site support centers perform depot support located at prime mission equipment repair facilities; and
- Integrated data management and communications links prime contractor support system together.

HUNTSVILLE MONITORING CENTER

7-15. The Huntsville monitoring center provides centralized management of all sustainment development program phase II resources and activities. Located in Huntsville, Alabama, at the prime contractor facilities, it is staffed by subject matter experts from all the prime offices. The material developer provides key interfaces for the Huntsville monitoring center and site managers for the operations center. Listed below are the principal functions and responsibilities of the Huntsville monitoring center:

- Coordinates the repair, replenishment, movement, inventory, distribution, and modification of all GMD prime mission equipment assets;
- Maintains support data on GMD assets including status and location;
- Provides scheduled and unscheduled maintenance information to the GMD operations center as required;
- Analyzes prime contractor support system sustainment performance data to determine improvement in the system effectiveness;
- Provides reports as required to government and prime contractor management;
- Provides centralized management of processes and procedures, acquisition control, transportation coordination, and authority for parts re-route;
- Provide training to personnel prior to deployment;
- Provides program administrators for sustainment management information systems, computerized inventory and maintenance management system, and training records databases;
- Collects maintenance data from sites, compiles reports, and distributes reliability, availability, and maintainability data and other analyses; and
- Maintains prime contractor support system metrics.

OTHER SUSTAINMENT OPERATIONS

7-16. GMD elements require continuous, reliable electrical power, air handling, and fire protection. Primary considerations are:

- Where possible, site utilities operate on commercial power, with an uninterruptible power supply with backup power generation. The extreme dependence of the system operation on both electrical power and cooling equipment requires sites have their own backup power generators.
- Heating, cooling, and ventilation must be available to support year-round continuous operations. Chemical, biological, radiological, and nuclear protection must be integral to the design of system operations facilities.
- Fire protection is an operational concern for GMD elements which must operate continuously. The unit must coordinate for fire protection and equipment which will not cause collateral damage to the system, and will allow the system to operate through all emergencies.
- Limited time operation by personnel within enclosed environments is possible, such as using breathing apparatus to accomplish emergency functions, as required.

UNIT READINESS

7-17. The GMD Commander ensures elements are operationally ready according to the potential for attack, the threat level, force protection for missile defense, information protection, operational area security, antiterrorism, survivability, chemical, biological, radiological, and nuclear, safety, and readiness condition. Soldiers must be ready to complete the GMD mission while managing many factors, such as routine maintenance, weather, training, and equipment upgrades. Ultimately, the commander participates in asset management conferences and has a voice in schedules and readiness decisions.

SUSTAINMENT REPORTING AND ACTIVITY PROCESSES

7-18. GMD operational reporting is conducted by FDC and MDE personnel for sustainment actions and situational awareness purposes. The FDC forwards equipment outage spot reports to the MDE. The MDE will initiate an asset management conference with key agencies to evaluate the impacts and effects to

operations capability. Immediately following the asset management conference, outages affecting operations and protection capabilities are reported and posted to all GMD agencies in accordance with USSTRATCOM Strategic Instructions.

7-19. The BMDS operational readiness reporting system is the system of record to collect BMDS operational readiness and system configuration data generated by the BMDS elements. It is a portal-based reporting and data collections system developed specifically to provide operational readiness and system configuration information for the BMDS. It accumulates operational readiness and system configuration information from data received within the operations support centers or from any BMDS site with access to their portal. The BMDS operational readiness reporting system asset list is maintained on a classified portal.

ARMY SUSTAINMENT FOR GROUND-BASED MIDCOURSE DEFENSE

7-20. The Army's sustainment objective is to ensure mission success. GMD elements must be operationally ready according to the force protection condition, and the readiness condition to defend against potential attack, Operations and sustainment are interdependent. Sustainment provides the commander the means to initiate and maintain operations at all levels of war.

SUSTAINMENT FUNDAMENTALS

7-21. The science of sustainment fundamentals for the Army also applies to GMD forces and integrates strategic, operational, and tactical sustainment efforts. The sustainment fundamentals include mobilization and deployment of units, personnel, equipment, and supplies in support of the GMD operations worldwide. Properly employed GMD forces allow a nation the freedom of action to deliver forces and materiel to the required points of application across the range of military operations from stability operations to major combat operations to successfully conduct those operations. A nation's capability to deliver logistic resources has historically been a major factor in military operations (JP 4-0).

7-22. During materiel acquisition, the Army requires critical systems be militarized, ruggedized, or hardened to operate reliably in environments subject to the effects of missile attacks. An example of hardening is the GMD tactical support facilities which must withstand electromagnetic pulse. Deployed forces must take steps to decrease their vulnerability to, or reduce the effectiveness of, an attack. For example, during deployment they may:

- Use site reconnaissance and selection, field fortifications, and dispersal;
- Implement post-attack recovery and reconstitution procedures; and
- Ensure critical functions and capabilities remain intact by using backup or alternate systems (redundant or robust means) to reduce vulnerability to attack.

OPERATIONAL CONTRACT SUPPORT AND THE LOGISTICS CIVIL AUGMENTATION PROGRAM

7-23. Other sustainment activities such as life support, theater transportation, and other functions not directly provided systems support contracts may also be required to fully sustain system deployments. Depending on the operational environment, the Logistics Civil Augmentation Program, or LOGCAP, is especially suited for key sustainment activities in support of personnel. Each Geographic Region has an existing LOGCAP task order that can be leveraged for support. LOGCAP is a strategic source for operational contract support and should be a preferred solution for sustainment activities that fall outside the scope of GMD support contracts. LOGCAP support can be accessed through the regionally aligned Army Field Support Brigade. For more information, see ATP 4-10.1.

FACILITIES

7-24. The Army must maintain support and facilities for GMD sites both within and outside the continental United States. For the Army facilities management and responsibilities, see AR 420-1.

7-25. Installation Management Command has responsibility for facilities and support. The basis for additional sustainment consideration outside the continental United States are the status-of-forces agreement or host nation agreement; these may augment the method of support provided by Installation Management Command.

7-26. Support and facilities for GMD sites outside the continental United States include mobile and fixed sites, missile defense complex, and support facilities:

- The base must be a closed area in the territory of the host nation used by United States forces pursuant to the provisions of the agreement for the purpose of deployment of GBIs. The base constitutes an agreed facility and area as defined in the United States-host nation supplemental status-of-forces agreement. The base corresponds to a United States installation.
- The missile defense complex is a restricted area, in accordance with USSTRATCOM Strategic Instructions. Restricted areas will be located within the military base or installation where all United States missile defense system components, support equipment, installation and maintenance is under United States control.
- GMD facilities are permanent structure built within the missile defense complex to house, operate, or support United States missile defense system operations.

GMD Mission Tactical Facilities

7-27. Mission tactical facilities are those facilities which contain, or are essential to, the operation of launch essential mission critical equipment and systems. The design of GMD facilities will meet specific operating requirements and environments. These requirements include:

- Power plant and utilities building;
- Fuel storage facility;
- Missile fields;
- Mechanical electrical building;
- IFICS data terminals;
- Readiness and control building; and
- Site infrastructure, such as communications, power, and water distribution lines which directly connects to or operates with launch essential mission critical equipment and systems.

GMD Mission Support Facilities

7-28. Mission support facilities are co-located with the tactical facilities in the launch farm complex and are required to operate and sustain those components. The design of facilities will meet the operating requirements and environments of the system being sustained. Baseline tactical sustainment facilities are:

- Administration and maintenance facility;
- Security monitoring and response facility;
- Entry control station;
- Logistic warehouse;
- Tank and de-tank facility (interceptor receiving facility);
- EKV fuel tank storage facility;
- EKV oxidizer tank storage facility;
- Interceptor storage facility;
- Water supply building;
- Waste water treatment facility; and
- General infrastructure, such as water, sewer, electrical, fire protection, fences, and parking areas.

Personnel

7-29. Soldiers and prime contractor personnel staff and maintain GMD systems for continuous 24-hour operations. The current approach for operational and support personnel will be qualified and certified military

personnel, and the maintenance and support personnel will be provided via a contractor logistics support concept. GMD forces consist of a mixture of active Army, ARNG, and AGR personnel and are commanded by a dual-status commander. Contract personnel fall under a chain of command established by the prime contractor.

7-30. The Army, in conjunction with the prime contractor and individual GMD components, specifies the quantities and skills of labor required for the BMDS element. Military personnel are expected to have completed their respective institutional resident training courses, been awarded their required Army military occupational specialty codes or area of concentration, upgraded their proficiency via on-the-job training and experience, and attended advanced residence courses. These individuals may occupy operations, maintenance, and support positions, to include operator, command, staff, instructor, and test functions. The military Services will certify personnel to their positions within the BMDS. Contractor personnel will be qualified and certified by their respective organizations on assigned positions and duties. Soldiers who operate the GMD fire control system are trained and certified in accordance with the GMD Gunnery Program.

7-31. During initial fielding of the AN/TPY-2 (FBM) radars, contractors operated and provided security at the first two AN/TPY-2 (FBM) locations. Security responsibilities for these two sites were transferred to the combatant command Army Service component command and these procedures are expected to be followed for future AN/TPY-2 (FBM) deployments. Site commanders have administrative control of the site but do not provide command or tactical control of the radar. Tactical control is normally exercised by the combatant command's Area Air Defense Commander through the AN/TPY-2 (FBM) detachment sensor managers using C2BMC.

7-32. Operating and maintaining the AN/TPY-2 (FBM) radar sites on a continuous basis has and will likely continue to rely largely on contractor support. The radar requires continuous 24-hour staffing. Any changes to the proper balance between military and contractor personnel will evolve by using lessons learned during initial operations, mission, enemy, terrain and weather, troops and support available, time available, civil considerations variables and other analysis.

MISSILE DEFENSE AGENCY

7-33. As the material developer, they keep combatant commands informed of the programs, plans, system capabilities, characteristics, limitations, and sustainment plans of GMD systems. They provide responses to requests for information and analysis in support of Army missile defense planning, operations, and sustainment. The Secretary of the Army signed an overarching memorandum of agreement between the MDA and the Army establishing the conditions for the transition and transfer of BMDS capabilities to the Army. The overarching memorandum of agreement addresses GBIs and ground BMDS.

7-34. Both the GMD fire control and AN/TPY-2 (FBM) radar systems are provided to the Army under limited material release guidelines. This allows the Army to field and operate the systems, but allows MDA to maintain configuration control and control the schedule for ongoing development. The plan for sustainment costs for the GMD and AN/TPY-2 (FBM) is for the Army service cell to execute the sustainment mission in accordance with Army regulations and policy. During limited material release transition, the GMD and AN/TPY-2 (FBM) product office will prepare and obtain Army approval of the supportability strategy. After the transfer, the Army will be responsible for sustainment costs not associated with configuration control and upgrades. A forum will prepare Army senior leaders for decisions in the program objective memorandum and budget. The Army funds through the program evaluation groups and the costs are used for internal planning and funding allocation processes.

7-35. Prior to deployment of any new or upgraded capability affecting Army forces, the MDA will provide a detailed briefing on the operational capabilities, limitations, and in-AOR support requirements. The purpose of these briefings is to identify the actions required to integrate improved capabilities within the existing mission command systems, support infrastructure, and to plan sustainment.

GROUND-BASED MIDCOURSE DEFENSE EQUIPMENT UPGRADES

7-36. The concept for the initial deployment was to include sufficient space, power, and air handling, allowing subsequent upgrades to occur without interference. After initial deployment, USNORTHCOM and

the GMD crew directors will be centrally involved in all systems upgrades to ensure current operations are not degraded and impacts to sustainment are examined.

7-37. Because the mission requires continuous operations, there will be closely managed windows of opportunity to shut down the system for routine and preventive maintenance. Performing maintenance in real-time without interference and before malfunctions cause secondary and tertiary faults is critical to the mission. Redundancy and multiple nodes in systems allow sub-elements to be off-line while performing maintenance. Managing maintenance windows for GMD equipment will be accomplished through the asset management process as outlined in USSTRATCOM Strategic Instructions.

7-38. The system requires certification testing of new hardware and software for fixes and upgrades. Any equipment or software connected to operations must be rigorously tested and certified before incorporation in the operational configuration. Since the systems cannot be shut down for testing, it is conducted on a non-interference basis.

This page intentionally left blank.

Source Notes

These are the sources quoted in this publication listed by page number.

1-1 "The new strategic challenges of the 21st Century require us to think differently . . ." National Security Presidential Directive 23, *National Policy on Ballistic Missile Defense*, 16 December 2002. Available at http://www.hsdl.org/?view&did=439067.

6-9 "The contemporary and emerging missile threat . . ." National Security Presidential Directive 23, *National Policy on Ballistic Missile Defense*, 16 December 2002. Available at http://www.hsdl.org/?view&did=439067.

This page intentionally left blank.

Glossary

The glossary lists acronyms and abbreviations and terms with Army or joint definitions, and other selected terms. Where Army and joint definitions are different, (Army) follows the term. Terms for which ATP 3-27.3 is the proponent (authority) manual are marked with an asterisk (*). The proponent manual for other terms is listed in parentheses after the definition.

SECTION I – ACRONYMS AND ABBREVIATIONS

AAMDC	United States Army Air and Missile Defense Command
AGR	Active Guard Reserve
AN/TPY	Army Navy/Transportable Radar Surveillance
AOR	area of responsibility
ARNG	Army National Guard
BDE	brigade
BMD	ballistic missile defense
BMDS	ballistic missile defense system
BN	battalion
C2BMC	Command and Control, Battle Management, and Communications
DOD	Department of Defense
DODD	Department of Defense directive
DS	defense strategy
ECF	entry control facility
EKV	exo-atmospheric kill vehicle
FBM	forward based mode
FDC	fire direction center
GBI	ground-based interceptor
GBMD	global ballistic missile defense
GMD	ground-based midcourse defense
ICBM	intercontinental ballistic missile
IFICS	in-flight interceptor communications system
IMD	integrated missile defense
IRBM	intermediate-range ballistic missile
JFCC	joint functional component command
LMS	launch management system
LOGCAP	Logistics Civil Augmentation Program
MD	missile defense
MDA	Missile Defense Agency
MDE	missile defense element

MDO	missile defense officer
NETOPS	network operations
NORAD	North American Aerospace Defense Command
OPCON	operational control
ROE	rules of engagement
RV	reentry vehicle
SATCOM	satellite communications
SBIRS	space-based infrared system (satellite)
SBX	sea-based x-band radar
SSL	security system level
UEWR	upgraded early warning radar
USASMDC	United States Army Space and Missile Defense Command
USNORTHCOM	United States Northern Command
USSTRATCOM	United States Strategic Command
XP	execution plan

SECTION II – TERMS

defense plan
Multiple defense designs combined together to create a cohesive plan for defending a broad area. (FM 3- 27)

deterrence
The prevention of action by the existence of a credible threat of unacceptable counteraction and/or belief that the cost of action outweighs the perceived benefits. (JP 3-0)

ground-based interceptor
(DOD) A fixed-based, surface-to-air missile for defense against long-range ballistic missiles using an exo-atmospheric hit-to-kill interception of the targeted reentry vehicle in the midcourse phase of flight. Also called GBI. (JP 3-01)

global ballistic missile defense
(DOD) Defense against ballistic missile threats that cross one or more geographical combatant command boundaries and requires synchronization among the affected combatant commands. Also called GBMD. (JP 3-01)

ground-based midcourse defense
(DOD) A surface-to-air ballistic missile defense system for exo-atmospheric midcourse phase interception of long-range ballistic missiles using the ground-based interceptors. Also called GMD. (JP 3-01)

rules of engagement
(DOD) Directives issued by competent military authority that delineate the circumstances and limitations under which United States forces will initiate and/or continue combat engagement with other forces encountered. Also called ROE. (JP 3-84)

References

All Web sites accessed on 21 October 2019.

REQUIRED PUBLICATIONS

These documents must be available to the intended users of this publication.

DOD Dictionary of Military and Associated Terms, July 2019.

ADP 1-02, *Terms and Military Symbols*, 14 August 2018.

RELATED PUBLICATIONS

These documents contain relevant supplemental information.

National Security Strategy, December 2017. Document is available at https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf

National Space Policy, 28 June 2010. Document is available at https://www.space.commerce.gov/policy/national-space-policy/

2013 Army Strategic Planning Guidance, 2013. Document is available at https://www.army.mil/e2/downloads/rv7/info/references/army_strategic_planning_guidance.pdf

DEPARTMENT OF DEFENSE PUBLICATIONS

CJCSI 3121.01B, *Standing Rules of Engagement/Standing Rules for the Use of Force for US Forces* (U), 13 June 2005. Document is available at https://www.jag.navy.mil/distrib/instructions/CJCSI%203121.01B13Jun05.pdf

Most DOD directives (DODD) are located on the DOD Issuance webpage located at: https://www.esd.whs.mil/Directives/issuances/dodd

DOD 5200.08-R, *Physical Security Program*, 9 April 2007.

DODD 5134.09, *Missile Defense Agency (MDA)*, 17 September 2009.

JOINT PUBLICATIONS

Most joint publications are available online from the Joint Doctrine Education and Training Electronic Information System (JDEIS) webpage at: https://jdeis.js.mil/jdeis

JP 3-0, *Joint Operations*, 17 January 2017.

JP 3-01, *Countering Air and Missile Threats*, 21 April 2017.

JP 3-12, *Cyberspace Operations*, 8 June 2018.

JP 3-27, H*omeland Defense*, 10 April 2018.

JP 3-30, *Joint Air Operations*, 25 July 2019.

JP 3-84, *Legal Support*, 2 August 2016.

JP 4-0, *Joint Logistics*, 04 February 2019.

JP 5-0, *Joint Planning*, 16 June 2017.

JP 6-0, *Joint Communications System*, 10 June 2015.

DEPARTMENT OF THE ARMY PUBLICATIONS

Most Army doctrinal publications are available online: https://armypubs.army.mil/

ADP 1, *The Army*, 31 July 2019.

ADP 3-0, *Operations*, 31 July 2019.

ADP 4-0, *Sustainment*, 31 July 2019.

ADP 6-0, *Mission Command: Command and Control of Army Forces*, 31 July 2019.

AR 10-87, *Army Commands, Army Service Component Commands and Direct Reporting Units*, 11 December 2017.

AR 190-11, *Physical Security of Arms, Ammunition, and Explosives*, 17 January 2019.

AR 190-13, *The Army Physical Security Program*, 27 June 2019.

AR 190-14, *Carrying of Firearms and Use of Force for Law Enforcement and Security Duties*, 12 March 1993.

AR 190-56, *The Army Civilian Police and Security Guard Program*, 15 March 2013.

AR 420-1, *Army Facilities Management*, 12 February 2008.

AR 750-1, *Army Materiel Maintenance Policy*, 3 August 2017.

ATP 3-12.3, *Electronic Warfare Techniques*, 16 July 2019.

ATP 3-27.5, *AN/TPY-2 Forward Based Mode Radar Operations*, 13 April 2015.

ATP 3-39.30, *Security and Mobility Support*, 30 October 2014.

ATP 3-39.32, *Physical Security*, 30 April 2014.

ATP 4-10, *Multi-Service Tactics, Techniques, and Procedure for Operational Contract Support*, 18 February 2016.

ATP 4-10.1, *Logistics Civil Augmentation Program Support to Unified Land Operations*, 01 August 2016.

ATP 5-19, *Risk Management*, 14 April 2014.

ATP 6-02.71, *Techniques for Department of Defense Information Network Operations*, 30 April 2019.

FM 3-12, *Cyberspace and Electronic Warfare Operations*, 11 April 2017.

FM 3-13, *Information Operations*, 6 December 2016.

FM 3-27, *Army Global Ballistic Missile Defense Operations*, 31 March 2014.

FM 3-39, *Military Police Operations*, 09 April 2019.

FM 6-27, *The Commander's Handbook on Law of Land Warfare*, 07 August 2019.

UNITED STATES CODE

These documents are available at http://www.loc.gov/law/help/guide/federal/uscode.php

United States Code, *Title 10 – Armed Forces.*

United States Code, *Title 32 - National Guard.*

United States Code, *Title 50 – War and National Defense*.

OTHER PUBLICATIONS

General Order Number 37, *Designation of the United States Army Space and Missile Defense Command/Army Strategic Command as an Army Service Component Command*, 16 October 2006. https://armypubs.army.mil/epubs/DR_pubs/DR_a/pdf/web/go0637.pdf

WEBSITES

Aegis Ballistic Missile Defense, 28 July 2016, https://www.mda.mil/news/fact_sheets.html

Army Navy / Transportable Radar Surveillance (AN/TPY-2), 28 July 2016, https://www.mda.mil/news/fact_sheets.html

Central Intelligence Agency. *Foreign Missile Developments and the Ballistic Missile Threat through 2015*. https://www.cia.gov/news-information/speeches-testimony/1999/walpole.htm

COBRA Dane Upgrade, 28 July 2016, https://www.mda.mil/news/fact_sheets.html

Command and Control, Battle Management, and Communications, 28 July 2016, https://www.mda.mil/news/fact_sheets.html

CRS Report for Congress, *Missile Survey: Ballistic and Cruise Missiles of Selected Foreign Countries Updated July 26, 2005 Strategy for homeland Defense and Civil Support: Department of Defense Washington, D.C.*, June 2006, http://www.dtic.mil/dtic/

Joint Functional Component Command for Integrated Missile Defense (JFCC-IMD), December 2011, https://www.stratcom.mil/components/

Missile Defense Agency, http://www.mda.mil

National Security Presidential Directive 23, *National Policy on Ballistic Missile Defense*, 16 December 2002. Available at https://www.hsdl.org/

Sea-Based X-Band Radar (SBX), 1 February 2018, https://www.mda.mil/news/fact_sheets.html

Unified Command Plan 2011, 6 April 2011. https://www.federalregister.gov/documents/2011/04/08/2011-8644/unified-command-plan-2011

Upgraded Early Warning Radars, AN/FPS-132, 28 July 2016, https://www.mda.mil/news/fact_sheets.html

USSTRATCOM Strategic Instructions, https://lynx.stratcom.smil.mil/rel/Publications/Lists/Publications/AllItems_copy(1).aspx

PRESCRIBED FORMS

This section contains no entries.

REFERENCE FORMS

Unless otherwise indicated, DA forms are available on the APD web site (https://armypubs.army.mil/).

DA Form 2028

Recommended Changes to Publications and Blank Forms.

This page intentionally left blank.

Index

Entries are by paragraph number, unless otherwise indicated.

1

100th Missile Defense Brigade, pg v, 1-29, 1-44 – 1-47, 2-10, 3-13, 3-17, 3-19, 3-27, 3-28, 3-33, 4-20, 5-15, 6-31, 6-44
Detachment 1-47, 3-27, 3-33, 6-44

4

49th Missile Defense Battalion, pg v, 1-29, 1-45 – 1-47, 2-11, 3-13, 3-19, 3-27, 3-28, 3-33, 4-20, 6-30, 6-32, 6-34, 6-39

A

Active defense, 3-14, 3-23, 6-53
Active Guard Reserve, 1-45, 1-46, 3-16, 3-20, 3-26, 3-27, 3-31, 6-24, 6-30, 7-28
Administrative control, 3-32, 7-30
Army Air and Missile Defense Command, 1-49, 1-50, 3-4, 3-5, 4-11
Army National Guard, pg iv, 1-45, 3-16, 3-18, 3-19, 3-27, 3-28, 3-31, 6-24, 6-30, 7-28
Army Service component command, 1-39, 6-30, 7-30, 7-33

B

BMDS communications network, 5-5, 5-6, 5-26
BMDS sensors, 2-47
  Aegis BMD, 2-39, 2-44 – 2-46, 3-22, 4-12, 4-14, 4-15, 5-7, 5-20
  AN/TPY-2 (FBM), pg v, 1-40, 1-41, 1-43, 1-50, 2-34 – 2-36, 2-48, 3-7, 3-13, 3-22, 3-24, 3-25, 4-11, 4-12, 4-14, 4-15, 4-44, 5-7, 5-18, 5-23, 6-42, 7-30, 7-31, 7-33
  COBRA Dane, 2-34, 2-37, 4-12, 4-14, 5-19
  SBX, 2-39 - 2-43, 4-12, 4-14, 5-21
  UEWR, 2-40, 2-44, 4-12, 4-14, 5-21

C

C2BMC, 1-41, 1-47, 1-48, 3-6, 3-7, 4-11, 5-7, 5-15-5-23, 7-30
C2BMC network interface processor, 5-18
Command and control 2-2, 3-1–3-14, 3-28, 5-2, 5-4, 5-13, 6-8, 6-53, 7-34
Commander's intent, 1-2, 2-4, 2-11, 3-1, 4-2–4-5, 4-8, 4-10, 4-16– 4-42, 6-36, 7-4
Contractor logistics support, 7-1, 7-6, 7-8, 7-12, 7-28
  prime contractor support, 6-16, 7-5–7-15, 7-28-7-29

D

Defended area, 1-46, 2-4, 4-4, 4-9, 4-12, 4-23 – 4-26, 4-36, 6-4
Defended asset list, 4-3, 4-26
Defense Strategy/Execution Plan, 2-3, 4-4, 4-5, 4-18, 4-22, 4-24, 4-26, 4-28, 4-36

E

Engagement planner, 2-4, 4-10, 4-13
Exo-atmospheric kill vehicle, 1-12 – 1-15, 2-2 - 2-5, 2-12, 2-24 - 2-29, 2-42, 4-10, 4-14, 5-22, 7-27
External system interface, 2-7, 5-20

F

Force protection condition, 4-19, 4-20, 6-21, 7-20

G

Global ballistic missile Defense, pg iv, 1-2, 1-3, 1-25, 1-26, 1-29, 1-43, 1-49, 1-51, 3-3 – 3-13, 4-2, 4-11, 5-25, 5-26, 5-29
GMD battle management, 1-4, 1-24, 1-41, 1-51, 2-2, 2-47, 3-6, 3-7, 4-10, 5-2, 5-23, 5-29
Ground-based Midcourse Defense
  employment guidelines, 4-22, 4-30
  engagement operations, 2-2, 2-30, 3-14, 3-23, 4-1, 4-8 - 4-18
  fire control nodes, 1-55, 1-46, 2-1, 2-8 – 2-12, 3-32, 4-37, 4-40, 5-8, 5-9, 5-20, 5-29, 6-56, 7-36
  fire control system, 1-12, 1-44, 2-2-2-9, 2-14, 2-33, 4-17, 4-18, 4-29, 4-31, 4-36, 4-42, 4-43, 5-8, 5-18, 7-29
Fire Direction Center, 1-46, 2-5, 2-8, 2-10, 2-11, 3-26, 3-33, 4-13, 5-20, 6-34, 7-18
GBI, pg v, 1-11 – 1-15, 1-47, 2-4, 2-12 – 2-28, 2-45, 4-6, 4-10 – 4-18, 4-34, 4-38, 4-42, 6-4, 6-29, 7-25, 7-32
GBI site security, 6-33 - 6-41
Missile Defense Element, 1-45, 1-46, 2-5 – 2-11, 3-26, 3-33, 4-9, 4-13, 5-15, 5-20, 7-18

H

Homeland defense, 1-9, 1-11, 1-36, 1-44, 1-50, 2-45, 2-46, 3-10 – 3-14, 3-18, 3-22 – 3-25, 6-46, 6-52

I

In-flight interceptor communications system, 1-12, 2-1, 2-5, 2-24, 2-29, 5-22, 7-26
Integrated tactical warning and attack assessment, 1-37, 2-33
Intercontinental ballistic missile, pg v, 1-1, 1-3, 1-8 – 1-11, 1-44, 1-46, 2-45, 3-22, 4-23, 4-24
Intermediate-range ballistic missile, 1-1, 1-3, 1-8 – 1-11

J

Joint forces component command
  JFCC IMD, 1-30, 1-31, 1-49, 3-10, 4-2, 5-5, 5-14, 5-24, 5-28

L

Logistics control center, 7-6

M

Missile fields, 2-11, 2-12, 6-16, 6-34, 7-26

Mission control station, 2-33, 5-17

N

NORAD, 1-37, 2-8

O

Operational environment, 1-16 thru 1-18, 4-22, 4-25
Organizations with a role in GBMD
  100th MD BDE (GMD), 1-29, 1-44 – 1-47, 2-10, 3-13, 3-17, 3-19, 3-27, 3-28, 3-33, 4-20, 5-15, 6-31, 6-44
  USASMDC, 1-3, 1-39, 1-40, 1-49, 3-3, 3-4, 3-15, 3-16, 3-27, 3-29, 3-32, 3-33, 4-44, 6-4, 6-30, 6-31, 6-32
USNORTHCOM, 1-7, 1-20, 1-37, 1-43-1-44, 1-46, 1-49, 2-8 thru 2-11, 3-7, 3-10, 3-12 thru 3-15, 3-22-3-23, 3-25, 3-26, 4-2, 4-9, 4-10, 4-20, 4-33, 4-34, 5-15, 5-20, 7-35
United States Indo-Pacific Command, 1-7, 1-46
USSTRATCOM, 1-3, 1-5, 1-7, 1-11, 1-34, 1-36–1-37, 1-39, 1-40, 1-44, 1-46-1-47, 1-55, 3-10, 3-13, 3-15, 4-2, 4-19, 5-15, 5-15, 5-24, 5-25, 6-2, 7-18, 7-36
Overhead persistent infrared, 2-37, 4-9, 4-12, 4-14
  DSP, 2-37–2-38, 4-9, 5-17
  SBIRS, 2-37 thru 2-39, 4-9, 5-7, 5-17

P

Prime contractor support system, 7-5, 7-12 thru 7-15

R

Readiness condition, 2-10, 4-19, 4-20, 7-17, 7-20
Reentry vehicle, 1-15, 1-16, 1-22, 2-31, 2-53, 4-15, 4-41
Rules of engagement, 4-7, 4-36, 4-39

S

Satellite communications, 5-6, 5-9, 5-10, 5-16, 5-18, 5-19, 5-21, 5-27
Security system level, 6-1-6-2, 6-6–6-7, 6-20, 6-23, 6-32, 6-37, 6-41
Sensor management operations, 2-44, 2-54, 2-55, 3-24, 4-11, 5-18
Sensor managers, 1-48, 5-23, 7-30
State governor/adjutant general force relationship, 3-28 thru 3-31
Submarine launch ballistic missile, 6-48

T

Threats
  asymmetric warfare, 6-55
  protesters, 6-5, 6-10, 6-13, 6-25, 6-54

U

US Code Title 10 and 32
  responsibilities, 1-50, 3-15 thru 3-20, 3-26 thru 3-33, 6-29

W

Weapons control status, 2-10, 4-13, 4-38
Weapons of mass destruction, 6-45, 6-47
Weapons release authority, 4-6, 4-9, 4-34, 4-38
Weapons task plan, 2-4, 2-13, 2-34, 4-38

ATP 3-27.3

30 October 2019

By Order of the Secretary of the Army:

JAMES C. MCCONVILLE
General, United States Army
Chief of Staff

Official:

KATHLEEN S. MILLER
Administrative Assistant
to the Secretary of the Army
1929715

DISTRIBUTION:
Distributed in electronic media only (EMO).

PIN: 106356-000