United States Government Accountability Office

Report to Congressional Committees

December 2019

MISSILE DEFENSE

Further Collaboration with the Intelligence Community Would Help MDA Keep Pace with Emerging Threats

GAO Highlights

Highlights of GAO-20-177, a report to congressional committees

December 2019

MISSILE DEFENSE

Further Collaboration with the Intelligence Community Would Help MDA Keep Pace with Emerging Threats

Why GAO Did This Study

MDA is developing missile defense capabilities to defend the United States, deployed forces, and regional allies from missile attacks. However, missile threats continue to emerge, as adversaries continue to improve and expand their missile capabilities.

The National Defense Authorization Act for Fiscal Year 2012 included a provision that GAO annually assess and report on the extent to which MDA has achieved its acquisition goals and objectives, and include any other findings and recommendations. This report is a public version of a classified report GAO issued in May 2019, which addresses (1) the challenges MDA and the defense intelligence community face in meeting the agency's threat assessment needs and (2) the extent to which MDA engages the defense intelligence community on missile defense acquisitions. GAO reviewed MDA's threat-related acquisition processes and interviewed relevant officials from the defense intelligence community, MDA, test community, and warfighters. Information deemed classified by DOD has been omitted.

What GAO Recommends

GAO is making three recommendations to improve how MDA: prioritizes and resources its threat assessment needs; obtains input from the defense intelligence community on key threat-related processes and decisions for missile defense acquisitions; and validates its threat models. DOD concurred with all three recommendations, citing actions it is already taking. While DOD has taken some positive steps, GAO believes more action is warranted.

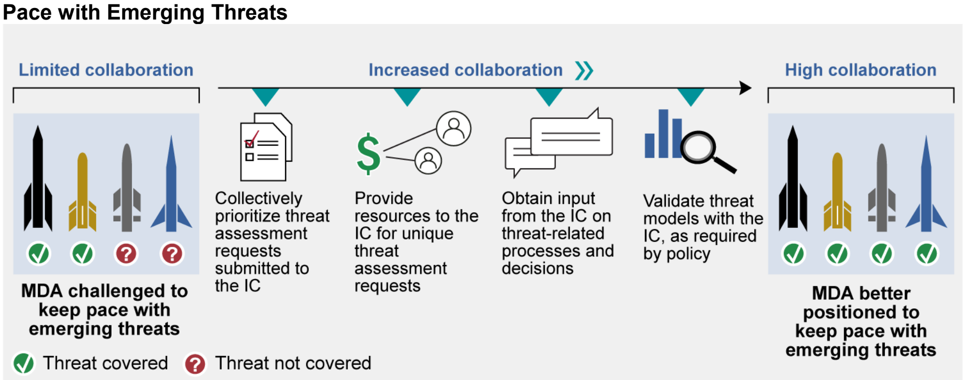
View GAO-20-177. For more information, contact Cristina Chaplain at (202) 512-4841 or chaplainc@gao.gov.

What GAO Found

The Missile Defense Agency (MDA) is experiencing delays getting the threat assessments needed to inform its acquisition decisions. Officials from the defense intelligence community—intelligence organizations within the Department of Defense (DOD)—told GAO this is because they are currently overextended due to an increased demand for threat assessments from a recent upsurge in threat missile activity, as well as uncertainties related to their transition to new threat processes and products. The delays are exacerbated because MDA does not collectively prioritize the various types of threat assessment requests submitted to the defense intelligence community or provide resources for unique requests, as other major defense acquisition programs are generally required to do. Without timely threat assessments, MDA risks making acquisition decisions for weapon systems using irrelevant or outdated threat information, which could result in performance shortfalls.

MDA has increased its outreach to the defense intelligence community over the past few years, but opportunities remain for further engagement on key threat-related processes and decisions. Specifically, MDA provides the defense intelligence community with limited insight into how the agency uses threat assessments to inform its acquisition decisions. MDA is not required to obtain the defense intelligence community's input, and instead has discretion on the extent to which it engages the defense intelligence community. However, the defense intelligence community is uniquely positioned to assist MDA and its involvement is crucial for helping MDA keep pace with rapidly emerging threats. Moreover, this limited insight has, in part, prevented the defense intelligence community from validating the threat models MDA builds to test the performance of its weapon systems. Without validation, any flaws or bias in the threat models may go undetected, which can have significant implications on the performance of MDA's weapon systems. MDA and the defense intelligence community recently began discussing a more suitable level of involvement in the agency's acquisition processes and decisions.

Actions Needed for MDA to Improve Collaboration with the Intelligence Community and Keep Pace with Emerging Threats


Limited collaboration
Increased collaboration
High collaboration
Collectively prioritize threat assessment requests submitted to the IC
Provide resources to the IC for unique threat assessment requests
Obtain input from the IC on threat-related processes and decisions
Validate threat models with the IC, as required by policy
MDA challenged to keep pace with emerging threats
MDA better positioned to keep pace with emerging threats
Threat covered
Threat not covered

IC = Intelligence Community, MDA = Missile Defense Agency

Source: GAO analysis of Missile Defense Agency and Intelligence Community data. | GAO-20-177

Note: the threat missile coverage depicted is notional and not representative of MDA's actual threat coverage.

Contents

Tables

Figures

Abbreviations

BMD	ballistic missile defense
BMDS	Ballistic Missile Defense System
CAPE	Cost Assessment and Program Evaluation
CRBM	close-range ballistic missile
DIA	Defense Intelligence Agency
DIBMAC	Defense Intelligence Ballistic Missile Analysis Committee
DOD	Department of Defense
DOT&E	Director, Operational Test and Evaluation
ICBM	intercontinental ballistic missile
IRBM	intermediate-range ballistic missile
MDA	Missile Defense Agency
MRBM	medium-range ballistic missile
NASIC	National Air and Space Intelligence Center
OTA	Operational Test Agency
SRBM	short-range ballistic missile
VOLT	Validated Online Lifecycle Threat
U	unclassified

GAO U.S. GOVERNMENT ACCOUNTABILITY OFFICE
441 G St. N.W.
Washington, DC 20548

December 11, 2019

Congressional Committees

The threat of ballistic missiles to the United States, deployed forces, and regional allies continues to increase, as indicated by recent missile tests by foreign adversaries that have demonstrated both increased capabilities and the potential to reach the United States. Ultimately, the challenge for the United States is how to contend with these foreign adversaries' threat capabilities, which are becoming more mobile, reliable, accurate, and capable of achieving longer ranges. The Department of Defense's (DOD) Missile Defense Agency (MDA) is working to address this challenge by developing the Ballistic Missile Defense System (BMDS) to detect, track, and defend against these threats to the homeland and abroad. MDA uses information on foreign adversaries' missile capabilities, which is primarily derived from threat assessments prepared by the defense intelligence community (Defense Intelligence Agency and the military services' intelligence production centers), to inform its BMDS acquisition decisions. Defense acquisition and intelligence leaders have recognized that greater consideration of threat capabilities in design and testing decisions throughout a weapon system's lifecycle can reduce developmental costs and operational risk.[1] With today's rapidly evolving threat capabilities, it is not only fiscally prudent to ensure that weapon systems are informed by defense intelligence community threat assessments, it is also vital to our national security, as each decision shapes future defensive capabilities.

Various National Defense Authorization Acts since 2002 have included provisions for us to prepare annual assessments of MDA's progress toward meeting its acquisition goals. Specifically, the National Defense Authorization Act for Fiscal Year 2012, as amended, included a provision for us to report annually on the extent to which MDA has achieved its acquisition goals and objectives, and include any other findings and recommendations on MDA's acquisition programs and accountability, as appropriate.[2] To date, we have issued 16 reports citing MDA's progress and challenges in developing and delivering the BMDS, including our

[1] Paul Reinhart and Brian Vanyo, "Improving Threat Support for DoD Acquisition Programs," *Defense AT&L,* Vol. XLVI, No. 3 (Ft. Belvoir, VA: May-June 2017).

[2] Pub. L. No. 112-81, § 232(a) (2011). The National Defense Authorization Act for Fiscal Year 2016 extended our reviews through fiscal year 2020. See Pub. L. No. 114-92, § 1688 (2015).

most recent report issued in June 2019.[3] For this review, we assessed (1) what challenges, if any, MDA and the defense intelligence community face in meeting the agency's threat assessment needs and (2) the extent to which MDA engages the defense intelligence community on BMDS acquisition. This report is a public version of a classified report that we issued May 1, 2019.[4] DOD deemed some of the information in our May 1, 2019 report as classified, which must be protected from loss, compromise, or inadvertent disclosure. Therefore, this report omits classified information on specific foreign adversary threats or threat space coverage by the BMDS. Although the information provided in this report is more limited, the report addresses the same objectives as the classified report and uses the same methodology.

To assess the challenges that MDA and the defense intelligence community face in meeting the demands for threat assessments, we reviewed summaries of meetings, requested responses from both MDA and the defense intelligence community via a questionnaire, and examined other documentary evidence. We compared this information to GAO best practices on inter-governmental agency collaboration, scheduling, and cost estimating.[5] We also interviewed officials from the defense intelligence community and MDA to better understand their perspectives on past and current collaboration, challenges and workload, and status and implications associated with recent revisions to threat assessment policies and processes.

[3] GAO, *Missile Defense: Delivery Delays Provide Opportunity for Increased Testing to Better Understand Capability*, GAO-19-387 (Washington, D.C.: June 6, 2019).

[4] GAO, *Missile Defense: Further Collaboration with the Intelligence Community Would Help MDA Keep Pace With Emerging Threats*, GAO-19-92C (Washington, D.C: May 1, 2019).

[5] GAO, *GAO Schedule Assessment Guide: Best Practices for Project Schedules*, GAO-16-89G (Washington, D.C.: Dec. 22, 2015); *Standards for Internal Control in the Federal Government*, GAO-14-704G (Washington, D.C.: Sept. 10, 2014); *Managing for Results: Key Considerations for Implementing Interagency Collaborative Mechanisms*, GAO-12-1022 (Washington, D.C.: Sept. 27, 2012); *GAO Cost Estimating and Assessment Guide: Best Practices for Developing and Managing Capital Program Costs*, GAO-09-3SP (Washington, D.C.: Mar. 2, 2009); *Best Practices: An Integrated Portfolio Management Approach to Weapon System Investments Could Improve DOD's Acquisition Outcomes*, GAO-07-388 (Washington, D.C.: Mar. 30, 2017); and *Results Oriented Government: Practices That Can Help Enhance and Sustain Collaboration among Federal Agencies*, GAO-06-15 (Washington, D.C.: Oct. 21, 2005).

To evaluate the extent to which MDA engages the defense intelligence community on BMDS acquisition, we identified the processes MDA has established for using defense intelligence community threat assessments to inform BMDS acquisition. To identify these processes, we reviewed relevant DOD and MDA policies, agency engineering documents, and briefings that either establish or provide overviews of the agency's threat-related requirements and processes, including threat model validation. We assessed MDA's implementation of its processes for incorporating threat assessments into its acquisitions by comparing the threat capabilities that the BMDS is being designed to defend against to those projected by the defense intelligence community. We omitted information on the threats that the BMDS is designed to defend against and other detailed information on threat capabilities throughout this report because it is classified. We discussed and corroborated our assessment of MDA's implementation of its processes with knowledgeable officials within MDA, the defense intelligence community, DOD test and evaluation offices, the military services, joint staff, and two major MDA contractors.

The performance audit upon which this report is based was conducted from February 2018 to May 2019 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives. We subsequently worked with DOD from May 2019 to December 2019 to prepare this unclassified version for public release based on the original classified report.[6] This public version was also prepared in accordance with these standards.

Background

Ballistic Missile Threats

Ballistic missiles, which foreign adversaries generally use as a deterrent or instrument of coercion, are becoming increasingly important weapons to support military and political objectives. These weapons continue to proliferate and show advances in mobility, reliability, in-flight maneuverability, accuracy, and ability to reach longer distances.

[6] GAO-19-92C.

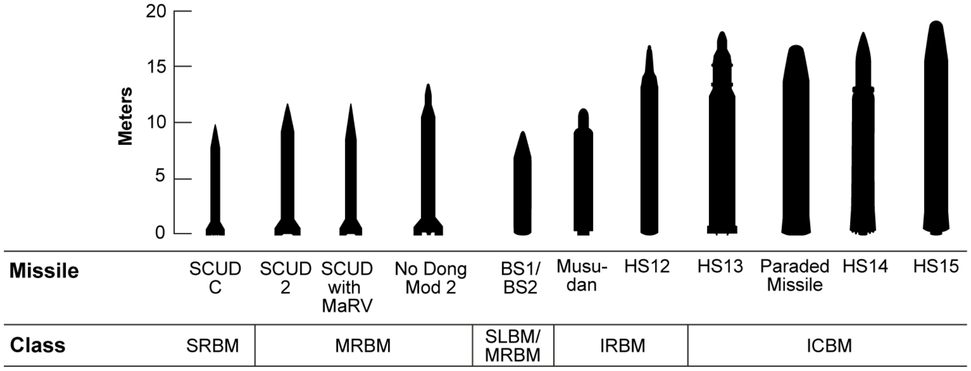
According to the defense intelligence community, there has been a dramatic increase in ballistic missile capabilities over the last decade, and the over 20 countries that already possess ballistic missiles are likely to pursue further expansions in their quantities and capabilities.[7] Figure 1 shows the lineup of operational ballistic missiles from North Korea and Iran, two of the various countries that pose threats to the United States and its allies and are of concern to the BMDS.

[7] National Air and Space Intelligence Center (NASIC) in collaboration with the Defense Intelligence Ballistic Missile Analysis Committee, *Ballistic and Cruise Missile Threat*, NASIC-1031-0985-17 (Wright-Patterson Air Force Base, Ohio: June 2017).

Figure 1: Ballistic Missiles of North Korea and Iran

North Korea

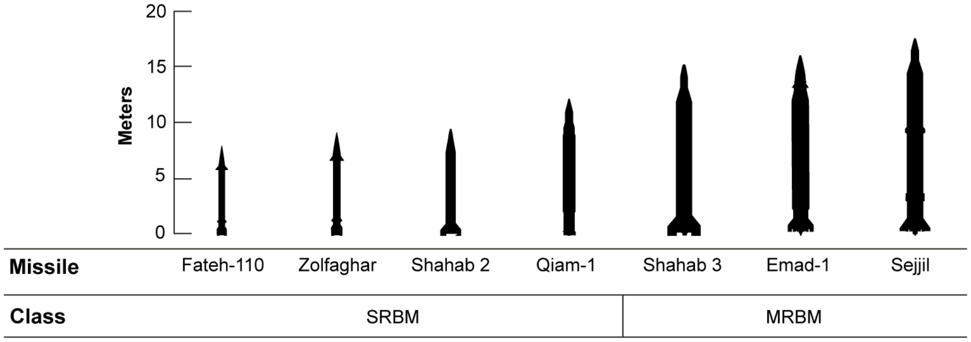
North Korea has an ambitious ballistic missile development program with an unprecedented pace of testing that has shown steady progress.



Missile	Class
SCUD C	SRBM
SCUD 2	MRBM
SCUD with MaRV	MRBM
No Dong Mod 2	MRBM
BS1/ BS2	SLBM/ MRBM
Musu-dan	IRBM
HS12	IRBM
HS13	ICBM
Paraded Missile	ICBM
HS14	ICBM
HS15	ICBM

Iran

Iran possesses the largest and most diverse arsenal of ballistic missiles in the Middle East. Iran has made recent strides to modify or develop ballistic missiles with improved range and precision. Iran is also pursuing a space program, which could provide it with a pathway to developing an intercontinental ballistic missile.



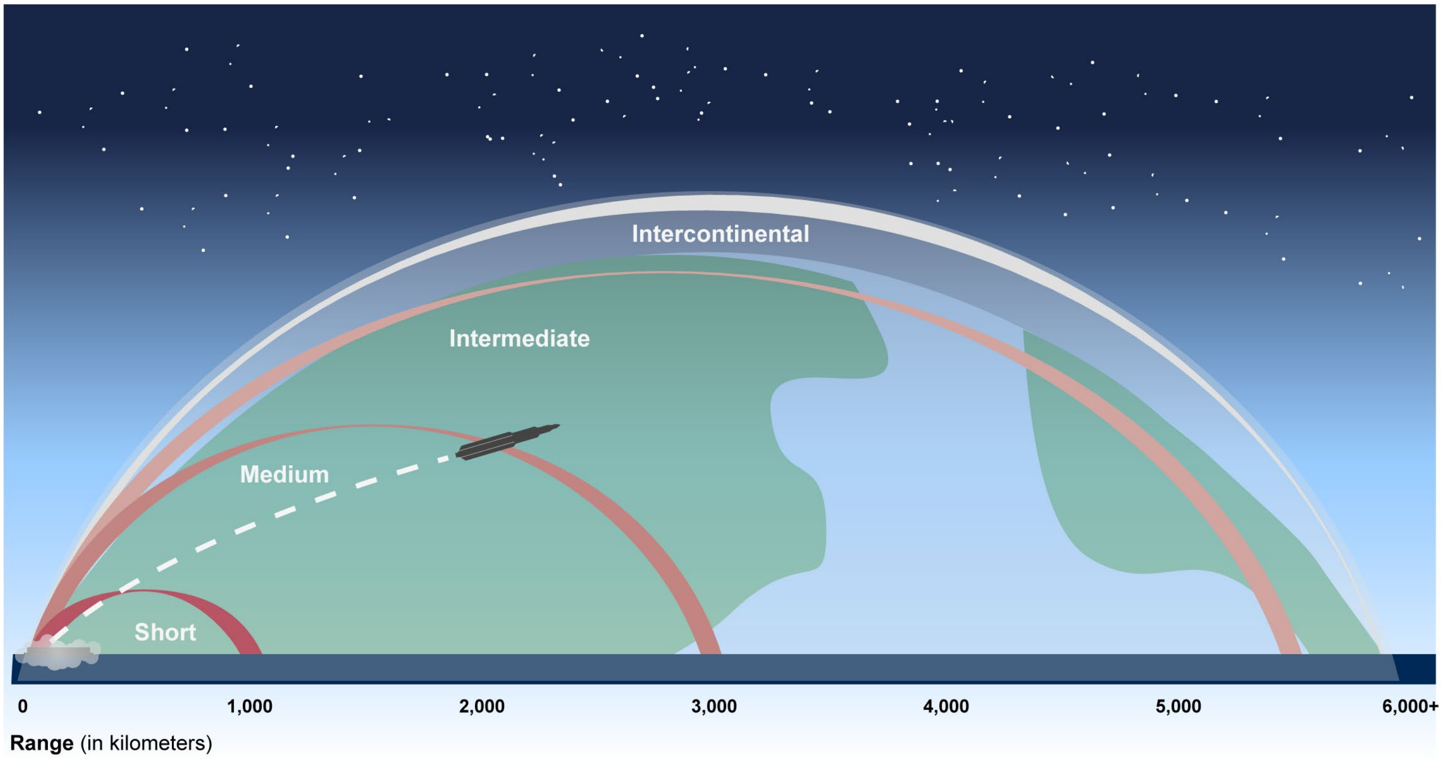
Missile	Class
Fateh-110	SRBM
Zolfaghar	SRBM
Shahab 2	SRBM
Qiam-1	SRBM
Shahab 3	MRBM
Emad-1	MRBM
Sejjil	MRBM

BS	Bukkeuseong
HS	Hwasong
ICBM	Intercontinental ballistic missile
IRBM	Intermediate range ballistic missile
MaRV	Maneuvering reentry vehicle
MRBM	Medium range ballistic missile
SLBM	Submarine launched ballistic missile
SRBM	Short range ballistic missile

Source: GAO presentation of defense intelligence community data. | GAO-20-177

Ballistic missile threats are generally categorized by their range (i.e., ground distance covered between the launch point and impact of the missile) as shown in figure 2 below.[8] The configuration of a ballistic missile is also largely determined by the range a missile is expected to travel. For example, longer range ballistic missiles typically have two or three distinct sections, known as stages, that separate during flight and each has an independent propulsion system to ensure the warhead reaches its target. Shorter range ballistic missiles generally only have one section, or a single stage, that remains intact until the warhead reaches its intended target and detonates.

Figure 2: Overview of Ballistic Missile Ranges



Source: GAO analysis of Missile Defense Agency data. | GAO-20-177

Note: This figure presents the maximum range for each missile class, although missiles are generally capable of achieving shorter ranges. Intercontinental ballistic missiles generally have a range greater than 5,500 kilometers.

[8] The intelligence community classifies ballistic missiles by range: close-range ballistic missiles (CRBM) are 50 - 300 kilometers; short-range ballistic missiles (SRBM) are 300-1,000 kilometers; medium-range ballistic missiles (MRBM) are 1,000-3,000 kilometers; intermediate-range ballistic missiles (IRBM) are 3,000-5,500 kilometers; and intercontinental ballistic missiles (ICBM) are greater than 5,500 kilometers.

Ballistic missiles may also carry countermeasures or adversaries may employ tactics and techniques, both of which are intended to confuse missile defense systems. For example, countermeasures can include penetration aids that are released during flight, such as decoys, which are intended to complicate the ability of missile-tracking sensors and missile defense interceptors to identify the warhead among the multiple objects. Challenging tactics and techniques can include structured attacks, such as simultaneously launching a number of missiles or outfitting a single missile with multiple warheads. In addition, some newer missiles are capable of traveling at greater speeds, performing maneuvers during all phases of flight, and remaining in the atmosphere for longer durations of their flight. These newer missiles, generally referred to as hypersonics, possess a combination of high speed, maneuverability, and relatively low altitude that can make them a challenging target for missile defense systems to track and engage. According to a publicly released intelligence assessment, nearly all adversaries that possess ballistic missiles have devised various means to confuse missile defense systems.[9]

Defense Intelligence Community's Roles in Assessing Missile Threats and Supporting MDA Acquisitions

In November 2010, the Defense Intelligence Agency (DIA) established the Defense Intelligence Ballistic Missile Analysis Committee (DIBMAC) to oversee and coordinate intelligence analysis and threat assessment production activities pertaining to foreign ballistic missile developments.[10] Under the leadership of this committee, the defense intelligence community performs important stakeholder, advisor, and oversight functions in support of MDA's acquisitions by (1) producing threat assessments; (2) providing advice on important threat-related issues pertaining to BMDS acquisition; and (3) validating threat models and reports. Table 1 provides further explanation of these roles and additional information on the defense intelligence community is in appendix I.

[9] NASIC, *Ballistic and Cruise Missile Threat*.

[10] DIA, *Memorandum to the Under Secretary of Defense for Intelligence, Action To Improve Ballistic Missile Analysis*, U-10-2464/CE (Washington, D.C.: Nov. 23, 2010).

Table 1: Defense Intelligence Community's Roles in Supporting the Missile Defense Agency

Stakeholder	**Producing Threat Assessments:** The defense intelligence community produces threat assessments for MDA with information on threat missiles and capabilities that MDA needs to inform Ballistic Missile Defense System (BMDS) acquisition decisions—design, development, and testing. The defense intelligence community gathers and assesses data from all available sources to ascertain the credibility, probability, and risks for a given threat, which it documents in different types of threat assessments.[a] The defense intelligence community manages a centralized database for MDA and others to request the different types of threat assessments, including the following: • **Country-specific threat assessments**—to include Validated Online Lifecycle Threat (VOLT) modules—contain all relevant threats and future projections for a specific country, which MDA uses to compile BMDS VOLT reports to inform design decisions. Under Department of Defense (DOD) policy, major defense acquisition programs are generally required to have a VOLT report, prepared by DOD components at specific points in their lifecycle, including, but not limited to, production decisions and operational testing.[b] According to DIA, VOLT reports only need to list the threat modules deemed relevant to the major defense acquisition program and the information can be supplemented, if necessary. • **Missile-specific threat assessments**—known as reference documents—include detailed technical information on a particular missile's size, performance characteristics, and signature when detected by a sensor, which MDA uses to build the threat models needed to design and test the BMDS.
Advisor	**Supporting Threat-Related Processes, Products, and Decisions:** The defense intelligence community is uniquely positioned to assist MDA on issues pertaining to threat missiles due to its mission, experience, expertise, and data sources. DOD policy requires MDA to coordinate with the defense intelligence community when addressing issues pertaining to the threat, such as intelligence implications of defensive capabilities.[c]
Oversight	**Threat Model Validation:** The Defense Intelligence Agency (DIA) is the validation authority for the threat models MDA uses to design, develop, and test the BMDS. Per DOD policy, all threat models and associated data must be validated by the DIA Director.[d] A threat model is a computer-based representation of a threat that replicates how the threat would perform in the real world. Model validation determines the degree to which the threat model accurately represents real-world performance based on the intended use(s) of the model. MDA conducts experiments—known as simulations—using threat models and models of its BMDS weapon systems to understand and gauge developmental progress and assess performance.[e] **VOLT Report Validation:** DIA also validates VOLT reports for major defense acquisition programs, including the BMDS. MDA uses threat modules from the defense intelligence community's digital threat library to compile VOLT reports to support BMDS acquisition decisions. DIA is responsible for ensuring that both the threat modules and VOLT reports are valid. VOLT report validation determines whether the report (1) includes appropriate and complete intelligence; (2) is consistent with existing intelligence positions, evidence, and analytic standards; (3) uses accepted analytic tradecraft in developing assessments; and (4) is compliant with relevant defense intelligence community directives.

Source: GAO analysis of DOD data. │ GAO-20-177

[a] Office of the Director of National Intelligence, Analytic Standards, Intelligence Community Directive 203 (Jan. 02, 2015); and DOD Directive 5105.21, DIA, (Mar. 18, 2008).

[b] DOD Instruction 5000.02, Operation of the Defense Acquisition System, (Jan. 7, 2015, Incorporating Change 3, August 10, 2017), p. 60. For other DOD acquisition programs, a VOLT report maps a single weapon system to all relevant threats regardless of country.

[c] DOD Directive 5134.09, Missile Defense Agency (MDA) (Sept. 17, 2009), pp. 9-10.

[d] DOD Instruction 5000.61, DOD Modeling and Simulation (M&S) Verification, Validation, and Accreditation (W&A) (Dec. 9, 2009), p. 6; and DOD Instruction 5000.02, p. 109.

[e] A simulation is a method for implementing a model and may include the use of digital devices, laboratory models, or “test bed” sites.

In November 2013, DOD’s acquisition leadership issued a memorandum that requested DIA work with the acquisition community to produce more timely, relevant, and dynamic defense intelligence community threat assessments for DOD acquisition programs.[11] The memorandum notes that DOD acquisition program officials expressed concerns about the timeliness of threat assessments due to the lengthy process and varying timelines that sometimes left them with threat assessments that did not contain the most up-to-date information. In addition, the defense intelligence community noted its concerns with the significant duplication in producing certain threat assessments, which placed a huge burden on its manpower and resources. Consequently, DOD leadership directed the acquisition customers and defense intelligence community to work together to improve threat assessments and in 2016 the defense intelligence community set forth its planned revisions to threat assessment processes and products.[12] Subsequent revisions include creating a library of threat modules and replacing a former type of threat assessment with a new Validated Online Lifecycle Threat (VOLT) report, among others. These revisions were codified in the defense intelligence community’s policies in September 2016 and in DOD policy in August 2017.[13] However, defense intelligence community officials noted that they are still in the process of implementing these revisions.

[11] Assistant Secretary of Defense for Acquisitions, *Memorandum for Director, Defense Intelligence Agency, Revitalization of System Threat Assessment Reports* (Washington, D.C.: Nov. 13, 2013).

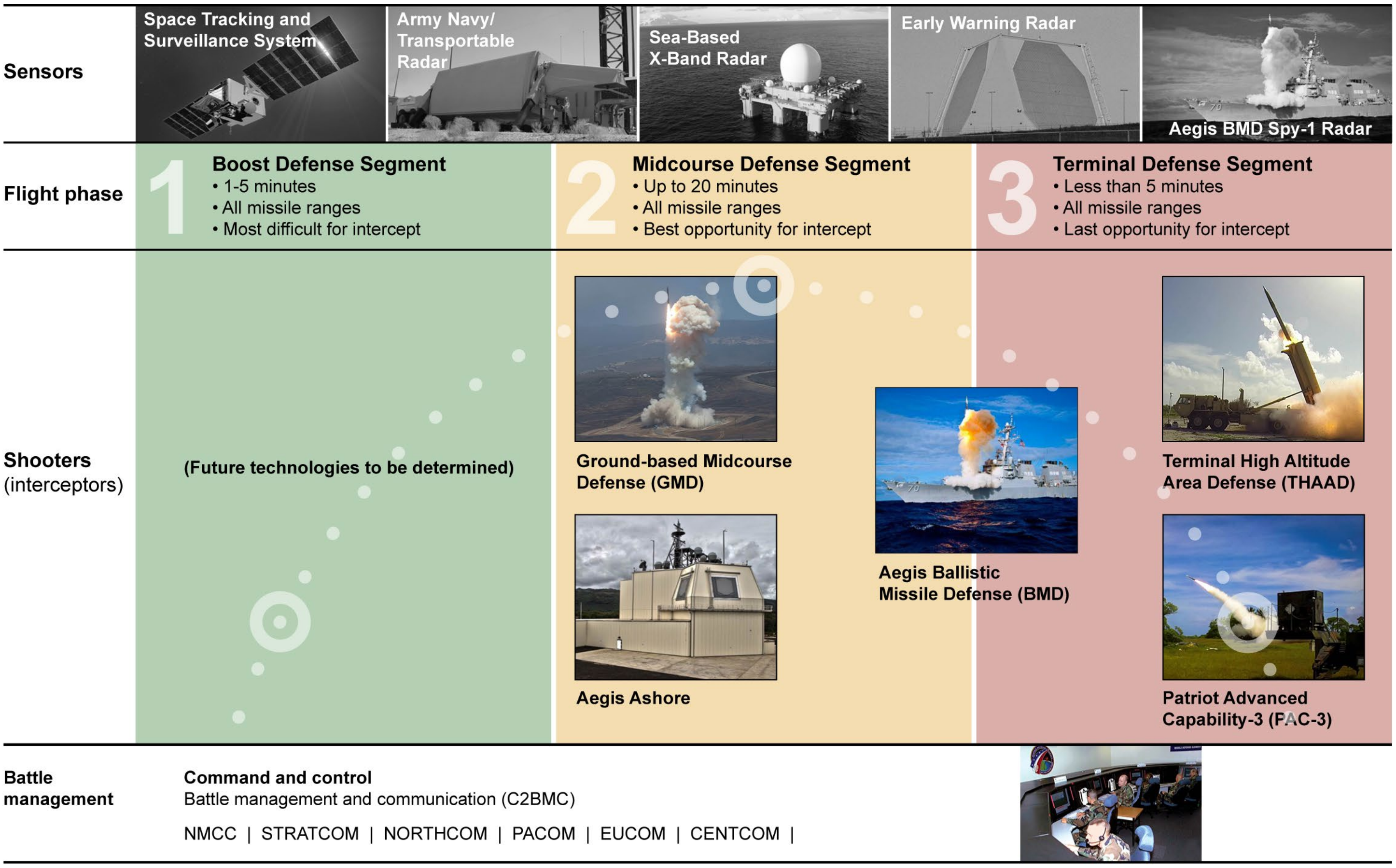
[12] Under Secretary of Defense for Acquisitions, Technology, and Logistics (AT&L), *Memorandum for Secretaries of the Military Departments, Deputy Chief Management Officer, DOD Chief Management Officer, Directors of Defense Agencies, and AT&L Direct Reports, Implementation Directive for Better Buying Power 3.0—Achieving Dominant Capabilities through Technical Excellence and Innovation* (Washington, D.C.: Apr. 9, 2015).

[13] DIA, Directive 5000.200, *Intelligence Threat Support for Major Defense Acquisition Programs* (Washington, D.C.: Sept. 19, 2016); and DOD Instruction 5000.02, *Operation of the Defense Acquisition System* (Jan. 7, 2015, Incorporating Change 3, August 10, 2017), p. 54, p. 60.

MDA's Responsibility for Defending Against Ballistic Missile Threats

MDA is developing a variety of missile defense systems, known as elements, including sensors, interceptors, and battle management and communication capabilities. The ultimate goal is to integrate these various elements to function as a layered system called the Ballistic Missile Defense System (BMDS). The BMDS elements, when integrated, are designed to destroy enemy missiles of various ranges, speeds, sizes, and performance characteristics in different phases of flight, as seen in figure 3 below.

Figure 3: Ballistic Missile Defense Architecture


Sensors
Space Tracking and Surveillance System
Army Navy/ Transportable Radar
Sea-Based X-Band Radar
Early Warning Radar
Aegis BMD Spy-1 Radar
Flight phase
1
Boost Defense Segment
• 1-5 minutes
• All missile ranges
• Most difficult for intercept
2
Midcourse Defense Segment
• Up to 20 minutes
• All missile ranges
• Best opportunity for intercept
3
Terminal Defense Segment
• Less than 5 minutes
• All missile ranges
• Last opportunity for intercept
Shooters (interceptors)
(Future technologies to be determined)
Ground-based Midcourse Defense (GMD)
Aegis Ashore
Aegis Ballistic Missile Defense (BMD)
Terminal High Altitude Area Defense (THAAD)
Patriot Advanced Capability-3 (PAC-3)
Battle management
Command and control
Battle management and communication (C2BMC)
NMCC | STRATCOM | NORTHCOM | PACOM | EUCOM | CENTCOM |

NMCC - National Military Command Center
STRATCOM - United States Strategic Command
NORTHCOM - United States Northern Command
PACOM - United States Pacific Command
EUCOM - United States European Command
CENTCOM - United States Central Command

Source: GAO analysis of Missile Defense Agency data and images. | GAO-20-177

When MDA was established in 2002, the agency was granted exceptional flexibilities to diverge from DOD's traditional acquisition lifecycle and defer the application of acquisition policies and laws designed to facilitate oversight and accountability until a mature capability is ready to be handed over to a military service for production and operational use. In particular, MDA was exempted from DOD's standard requirements-setting process and instead uses a unique and flexible requirements-setting process that is intended to enable MDA to quickly develop and field useful but limited capabilities, which can be incrementally improved over time and adapted to address changes in the threat.

MDA also implemented a tailored process that is intended to use defense intelligence community threat assessments in a way that enables the BMDS to defend against a broad range of uncertain and evolving threats. MDA uses defense intelligence community threat assessments as the foundation for developing threat models and establishing wide-ranging critical threat parameters upon which to design, develop, and test the BMDS.[14] Specifically, MDA's process includes the following:

- **Design:** MDA uses threat assessments to select a set of threat models in which it incrementally designs BMDS capabilities to defend against. MDA combines the capabilities from the selected threat models into parameters, forming what MDA refers to as the "parametric threat space." MDA assigns subsets of the threat space to each of the BMDS elements to inform the design of their respective systems.
- **Development:** MDA assigns specific threat models to each of the elements for use in simulations as they are undergoing development. MDA uses these threat models to verify that the element's system design has the capability necessary to defend against its assigned threat space.
- **Test:** Toward the end of BMDS element development, MDA coordinates with the warfighter and test and evaluation communities to select specific threat models for use in testing to assess the performance of the BMDS elements. MDA also uses its threat models to prepare for flight tests to help ensure that the BMDS elements have

[14] MDA produces a common set of threat models, threat specifications, and scenario data for use in BMDS development. Adversary capability is characterized using trajectory and signature models and data. Our use of the term "threat model" in this report generally refers to all of these items.

a high probability of achieving their test objectives, such as successfully intercepting the target.

- **Operational capability:** MDA uses its threat models as the foundation for algorithms, which are embedded into the BMDS to enable its sensors and interceptors to determine which object(s) amongst a group of objects (e.g., countermeasures, debris, etc.) is lethal. This capability is referred to as "discrimination."

Mounting Challenges Are Delaying the Availability of Threat Assessments, but Opportunities Exist to Help MDA Receive the Information It Needs

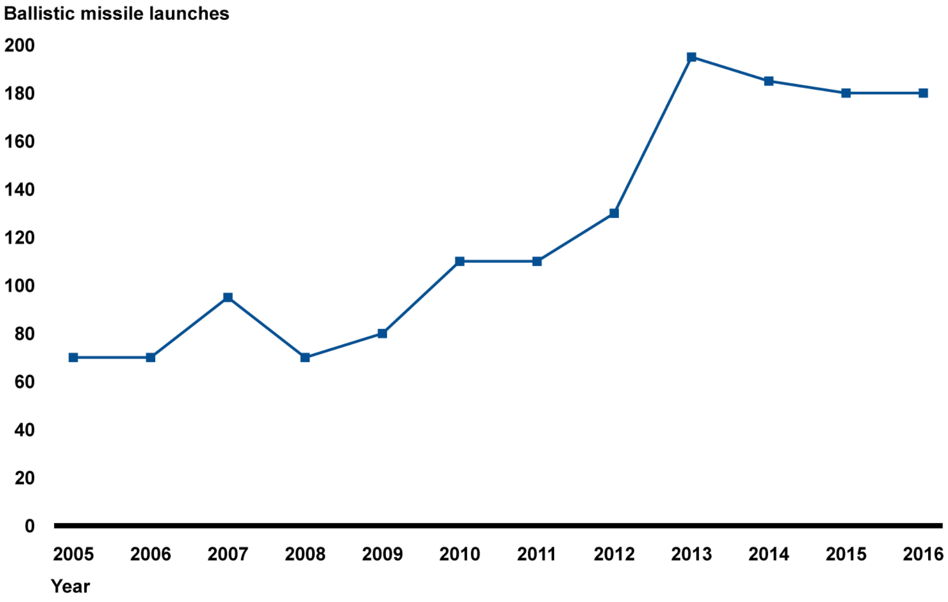
Various challenges have recently emerged that have affected the availability of the threat assessments MDA needs to inform the agency's acquisition decisions. Challenges include an upsurge in threat missile activity, which has increased the overall demand for threat assessments; a transition period as the defense intelligence community works through how to implement recent revisions to its processes and products; and MDA's request for accelerated support from the defense intelligence community. Defense intelligence community officials say they are contending with all of these challenges without the provision of additional manpower or resources. Consequently, defense intelligence community officials have stated that their manpower and resources are constrained, which can affect the timely delivery of threat assessments to customers, such as MDA. If MDA does not have the threat information it needs when it is needed, the delay of information could result in setbacks for the agency's weapon system design, development, and testing, or could put the agency in the position of moving forward without the requisite information, thereby increasing the risk of performance shortfalls and costly retrofits. However, MDA has opportunities to mitigate these challenges by collectively prioritizing its threat assessment requests and working through existing venues with the defense intelligence community to determine what additional resources may be needed to secure the accelerated support that it needs.

Various Challenges Are Delaying the Availability of Defense Intelligence Community Threat Assessments MDA Uses for Acquisition Design and Testing Decisions

Increased Threat Activity

One challenge for the defense intelligence community is a recent upsurge in threat missile activity, which has increased MDA's requests for threat assessments. For example, ballistic missile flight testing has more than doubled from 2005 to 2016, from about 70 tests in 2005 to nearly 180 tests in 2016, and the most notable increases have occurred since 2010 (see figure 4).

Figure 4: Ballistic Missile Flight Testing, 2005-2016



Source: GAO presentation of defense intelligence community data. | GAO-20-177

Note: The number of flight tests in this graphic is approximated. This graphic is based on a publicly released threat assessment from the defense intelligence community and substitutes the original graphic, which has been omitted due to classification.

This upsurge of threat missile activity increases the urgency for the defense intelligence community to provide the requisite type of threat assessments to MDA to enable the agency to counter and defeat such threats; however, defense intelligence community officials have said that manpower and resource constraints have limited their ability to do so. In 2016, we reported on how the defense intelligence community's manpower and resource constraints have impacted its ability to provide threat assessments.[15] Since then, defense intelligence community officials have said that the manpower and resource constraints have not been resolved, but threat missile activity has increased. For example,

[15] Citation to the GAO report has been omitted due to classification.

some countries have recently displayed or flight tested new threat missiles capable of reaching the United States. When new threat missiles emerge, MDA requests missile-specific threat assessments—known as reference documents—from the defense intelligence community to understand their size, performance characteristics, and signature when detected by a sensor. This detailed information on the threat missiles enables MDA to build the threat models used to design, develop, and test BMDS weapon systems.

Defense intelligence community officials have said that, although important, missile-specific threat assessments utilize considerable manpower and resources because they can be labor-intensive, lengthy, and take months, and at times a year or longer, to prepare. According to these officials, one way to minimize the workload and shorten the preparation timeframe is for MDA to differentiate the specific information that it needs from anything that might be extraneous. As a simplified and hypothetical example, defense intelligence community officials explained that MDA may only need some simple, general information about a missile or conversely it may need complex, highly-detailed information on everything about the missile from tip to tail. The amount of time and effort it would take defense intelligence community officials to gather the information in these two scenarios would vary significantly. MDA officials have acknowledged that some extraneous information may be gathered and included in these threat assessments but noted that, at the time they request a threat assessment, they may not yet fully understand what information is essential for their purposes. Therefore, they prefer to have as much information as possible, with the ability to determine whether and how to use it. Defense intelligence community officials, however, told us that they believe this is an inefficient use of their manpower and resources, especially given current constraints.

Revisions to Processes and Products

Another challenge for the defense intelligence community is the implementation of recent revisions to its threat assessment processes and products, which apply to all DOD acquisition programs. In 2016, in response to the November 2013 memorandum from DOD's acquisition leadership, the defense intelligence community began overhauling its threat assessment processes and products to produce more timely, efficient, and relevant information.[16] See table 2 for an overview of these revisions.

Table 2: Revision to Defense Intelligence Community's Threat Assessment Processes and Products

Revision	Creating a digitized library of threat modules.	Replacing a former type of threat assessment with the new Validated Online Lifecycle Threat (VOLT) report.
Description	Collection of 300 topic-area threat modules (e.g., electronic warfare, air-to-air missiles, adversary tactics, etc.) with 20 year projections for technologies and trends.	Primary threat document for an acquisition program, which includes an adversary country's strategy, tactics, current and projected force levels, weapon system descriptions and performance, technology trends, and proliferation.
Potential benefit(s)	Reduces duplication and inefficiency by replacing disparate reports with standardized modules that can be used across multiple threat assessments, DOD components, and acquisition programs. Improves timeliness of acquisition decision-making, as affected DOD components and acquisition programs receive instantaneous and simultaneous threat updates.	Improves relevance and value by being more future-focused and predictive, rather than historical. Less time-consuming to construct, because they are built using the digitized threat models.

Source: GAO analysis of DOD data. | GAO-20-177

While each of these revisions has potential benefits, defense intelligence community officials have said that implementing the revisions has been more time-consuming and difficult than anticipated, which has affected their ability to provide certain threat assessments to MDA when needed. For example, MDA and the defense intelligence community were initially uncertain about the responsibilities and processes for creating a VOLT report for the BMDS. Although it took some time to resolve these uncertainties, MDA is now compiling its own country-specific threat assessments—known as the BMDS VOLT report—which DIA then validates.[17] The military services generally have their own defense intelligence production centers, and therefore, a means for compiling VOLT reports. MDA, however, uses information from multiple defense intelligence production centers and does not possess its own production center. In September 2017, MDA reached out to DIA on this matter and DIA responded that, per the DOD policy update, it does not see anything that would preclude MDA, as a DOD component, from compiling VOLT

[16] Assistant Secretary of Defense for Acquisitions, *Memorandum for Director, DIA, Revitalization of System Threat Assessment Reports* (Washington, D.C.: Nov. 13, 2013).

[17] DOD Instruction 5000.02, p. 60.

reports.[18] DIA stated that MDA compiling its own VOLT report aligns the agency with the rest of the DOD acquisition community.

MDA is waiting on threat modules from the defense intelligence community to prepare its preliminary BMDS VOLT report, which MDA will use to inform acquisition decisions. MDA needs specific threat modules from the defense intelligence community, including those for six specific countries, in order to compile its preliminary BMDS VOLT report. However, defense intelligence community officials have said that they are still in the process of creating some of the digitized threat modules MDA needs, because it has taken more time and effort than they expected to standardize the threat modules' content and coordinate production across multiple defense intelligence community production centers. Consequently, MDA is planning to publish its preliminary BMDS VOLT report in 2019 (table 3).

Table 3: Completion Status of the Missile Defense Agency's (MDA) Validated Online Lifecycle Threat (VOLT) Report

Country included in MDA's VOLT report[a]	Year last threat assessment published[b]	Year MDA submitted request for updated threat assessment	Year MDA projects completion of new threat assessment[c]
Country one	2014-2016	2016-2017	2019
Country two			
Country three			
Country four			
Country five			
Country six			

Source: GAO presentation of defense intelligence community data. | GAO-20-177

[a]Specific country names have been omitted from this table due to classification.

[b]The 2014-2016 threat assessments in this table refer to specific documents that the defense intelligence community previously tailored to support MDA's acquisition baseline for the Ballistic Missile Defense System (BMDS). The Defense Intelligence Agency (DIA) is in the process of replacing these documents with digitized threat modules, because it determined that it did not have sufficient resources to sustain two threat assessment production processes in tandem.

[18]DIA, *MDA Request for a DIA Review of Department of Defense References Related to Validated Online Lifecycle Threat (VOLT),* U-108-17/TLA-3 (Washington, D.C.: Nov. 16, 2017). The *DOD Dictionary of Military and Associated Terms* (June 2018) defines a DOD component as all entities in DOD, including the Office of the Secretary of Defense, military services, Chairman of the Joint Chiefs of Staff and Joint Staff, combatant commands, Office of Inspector General, defense agencies, and field activities.

[c]MDA is using the threat modules prepared by the defense intelligence community to compile a consolidated BMDS VOLT report. The consolidated BMDS VOLT report will be validated by DIA, as required by policy.

In the meantime, without the preliminary BMDS VOLT report or digitized threat modules used to compile the BMDS VOLT report, MDA is reliant on threat assessments written between 2014 and 2016 for some of its acquisition decisions. For example, MDA recently made design decisions for certain BMDS elements using these threat assessments, although these threat assessments have not yet been updated.[19] Consequently, these weapon systems that MDA recently made design decisions for could have capability gaps or performance shortfalls that present risks for the warfighter. MDA has attempted to fill the void for digitized threat modules and the preliminary BMDS VOLT report by submitting *ad hoc* requests for threat assessments to the defense intelligence community, but this has only added to the defense intelligence community's workload and exacerbated delays.

Request for Accelerated Delivery of Threat Modules

Moving forward, MDA has asked the defense intelligence community to provide the digitized threat modules on an accelerated schedule to ensure the agency can compile BMDS VOLT reports in a timely manner to inform its acquisition decisions; however, some defense intelligence production centers have said that an accelerated schedule will be difficult, if not impossible, without additional manpower and resources. Specifically, MDA wants the defense intelligence community to provide the digitized threat modules every year, as opposed to every two years as required by DOD policy.[20] MDA has stressed the importance of having these digitized threat modules on an accelerated schedule in order to be responsive to threat advancements and mitigate the potential for capability gaps or performance shortfalls in its weapon systems. Defense intelligence community officials have acknowledged MDA's need to have the digitized threat modules on an accelerated schedule but are concerned about their ability to provide them due to personnel and resourcing issues at some defense intelligence production centers. For example, two defense intelligence production centers have said that MDA's request for an accelerated schedule is currently unrealistic due to their manpower and resource levels. Defense intelligence officials have said that once the initial digitized threat modules are created, the threat

[19] The specific weapon systems in this example have been omitted due to classification.

[20] DOD Instruction 5000.02, p. 54.

modules will be easier and quicker to update, but whether they can provide them annually is still being determined.

Opportunities Exist That Could Help MDA and the Defense Intelligence Community Address Threat Assessment Availability Challenges

Although MDA has the capability to centrally and collectively prioritize its threat assessment requests submitted to the defense intelligence community, it currently prioritizes its threat assessment needs through two distinct, individual lanes—country-specific and missile-specific—supplemented by informal discussions with the defense intelligence community. According to MDA, the individual lanes are as follows:[21]

1. **Country-specific threat assessments** (i.e., threat modules for BMDS VOLT reports) are prioritized via the VOLT Threat Steering Group, which is co-chaired by MDA and DIA. The VOLT Threat Steering Group's objectives are to determine MDA's threat module requirements, to achieve concurrence on the threat modules used in the BMDS VOLT report, and to review the BMDS VOLT production schedule. The first VOLT Threat Steering Group meeting was held in April 2018 and during that meeting, MDA presented its prioritized list of threat assessments by adversary country to the defense intelligence community personnel in attendance.
2. **Missile-specific threat assessments** (i.e., reference documents used to build threat models) are prioritized via an annual intelligence mission data process managed by the Joint Staff.[22] Through the intelligence mission data process, MDA prioritizes the data it needs for threat missiles by most to least critical—119 total threat missiles in 2018.

With these two individual lanes for prioritization, MDA treats each type of threat assessment as independent and unrelated. According to MDA, the

[21] For the purpose of this report, threat assessments are described as two particular types—country-specific and missile-specific. However, DIA generally does not use these terms to describe the intelligence products or support that it provides to major defense acquisition programs.

[22] Intelligence mission data characterizes technical features and attributes of missiles, such as associating a specific signature with an adversary's system. Signatures are distinct, repeating characteristics, such as radio frequencies or acoustic characteristics, which are associated with a particular type of equipment, materiel, activity, individual, or event. Intelligence missile data are essential for building system models, developing algorithms, optimizing sensor design, system testing and evaluation, and validating sensor functionality.

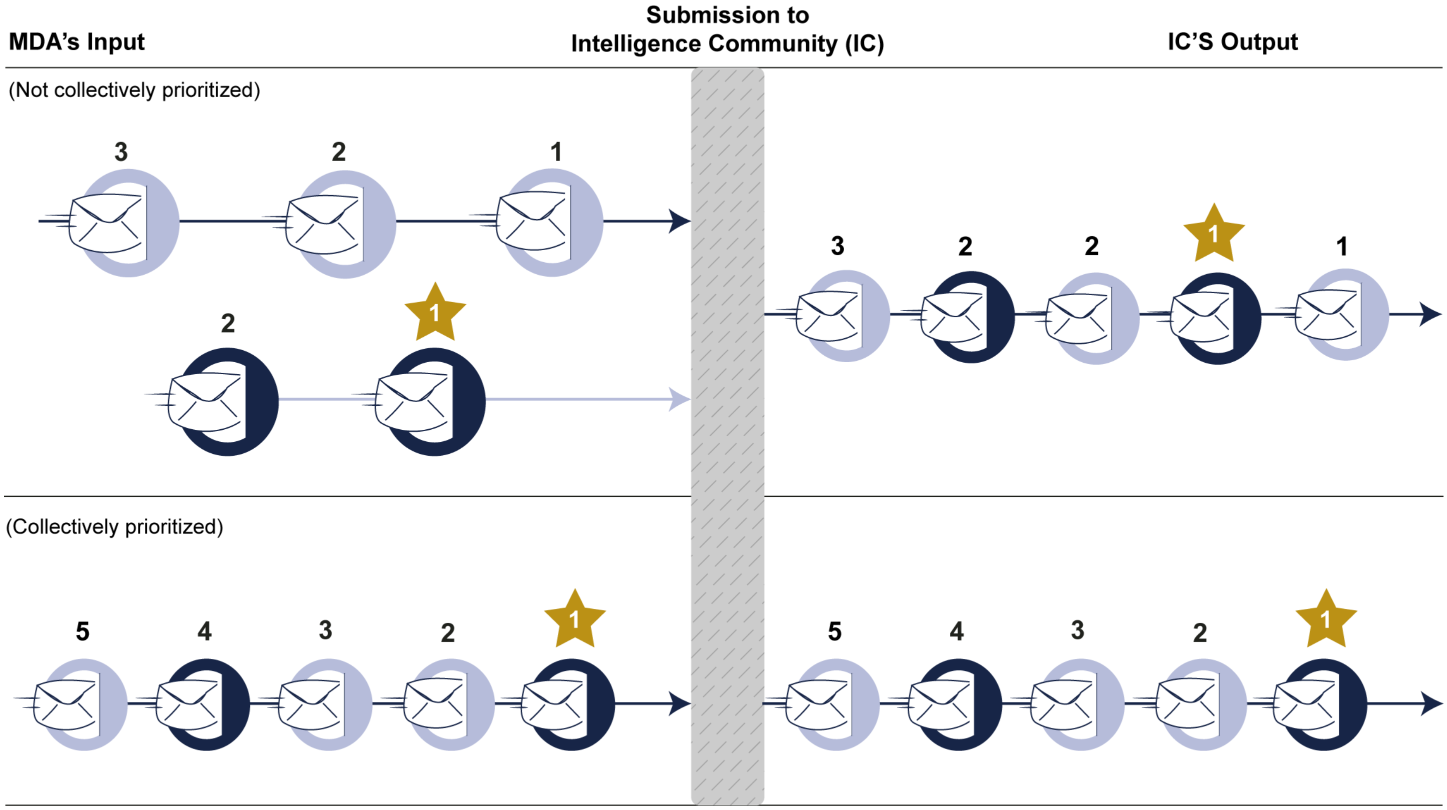
agency maintains these individual lanes for prioritizing its threat assessment requests because the requests can be more easily managed by the defense intelligence community components that develop the threat assessments. For example, MDA stated that requests for missile-specific threat assessments are often routed to intelligence production centers while requests for country-specific threat assessments are often routed to DIA’s regional centers (see appendix I for more information on defense intelligence community components). According to MDA, the vast majority of new requirements submitted to the defense intelligence community are also accompanied by an informal verbal discussion and if MDA’s priorities shift because a new threat emerges, MDA stated that it can convey that shift to the defense intelligence community in an effort to work out the best path forward.

If the defense intelligence community cannot meet MDA’s needs, MDA stated that it works with the defense intelligence community to determine the best course of action for resolving prioritization issues. For example, MDA cited a recent example where it had worked with the U.S. Navy’s Office of Naval Intelligence to develop a threat model production schedule for two threat systems; however, the emergence of a new threat shifted MDA’s priorities. MDA was able to understand the effect of choosing one system ahead of the others based on the priority and projected production timelines. MDA cited another recent example where it had similarly worked with the U.S. Air Force’s National Air and Space Intelligence Center to prioritize production of a threat model for a new, unique threat. After some initial informal discussions and questions about whether the threat model production effort was a top priority for MDA, both agreed in a meeting in January 2019 to lower the priority for the model production effort. The specific threats referenced in the examples above have been omitted because they are classified.

However, MDA’s approach of prioritizing its threat assessment needs through individual lanes creates the potential for unresolved, competing priorities because the defense intelligence community produces threat assessments collaboratively rather than disparately. Defense intelligence community officials told us that the underlying analyses that support both country-specific and missile-specific threat assessments are developed and reviewed by many of the same subject matter experts and managers within the defense intelligence community. Defense intelligence community officials told us that they have no way of knowing whether the information to build a specific threat model is a greater or lesser priority than updating a particular threat module needed to support the BMDS VOLT report. Our prior best practices work found that successful commercial companies employ a formal process for prioritizing their investments collectively rather than as independent and unrelated initiatives.[23] MDA instead stovepipes its threat assessment prioritization through individual lanes and informally discusses its collective priorities with the defense intelligence community. Consequently, MDA's requests, and resulting output from the defense intelligence community, may not be based on the collective order of importance, as depicted in figure 5.

[23] GAO-07-388.

Figure 5: Missile Defense Agency's (MDA) Potential to Collectively Prioritize Threat Assessment Requests in the Intelligence Community's Queue


MDA's Input
Submission to Intelligence Community (IC)
IC'S Output
(Not collectively prioritized)
3
2
1
2
1
3
2
2
1
1
(Collectively prioritized)
5
4
3
2
1
5
4
3
2
1

★ Most important threat assessment request

● Country-specific request (threat module for Validated Online Lifecycle Threat report to support design decision)

○ Missile-specific request (reference document to build threat model used in testing)

Source: GAO representation of MDA and intelligence community processes. | GAO-20-177

MDA relies on both country- and missile-specific threat assessments for its acquisitions, as each characterizes threats in unique ways and for different purposes, and it uses other requests to fill information gaps, as needed. Thus, all of MDA's requests are important, but one among them may be the most important or urgent due to the timing of an upcoming design or testing decision. In the example illustrated above in figure 5, the most important request is for a country-specific threat assessment; however, it will not likely be the next one out of the defense intelligence community's queue because there is a missile-specific request ahead of it. Hence, MDA may have the information it needs to build the threat model used to test one weapon system's performance, but it may delay the country-specific information it needs to make design decisions for another. This delay in the country-specific information could put MDA in a position of moving forward with design decisions without the requisite information or relying on outdated information, which increases the risk for performance shortfalls and costly retrofits.

One opportunity that MDA has to address the availability of threat assessments from the defense intelligence community is to collectively prioritize its threat assessment requests based on the order of importance. We have previously identified collective prioritization as a best practice—specifically, that it is important for an agency to regularly evaluate the totality of its needs or tasks, to determine whether specific ones should be prioritized ahead of others, based on the costs, benefits, and risks.[24] While MDA has no formal requirement to collectively prioritize its threat assessment requests, defense intelligence community officials said that they have had discussions with MDA through existing venues and requested that it do so to ensure it has the most urgently needed information.

MDA has the capability to collectively prioritize its threat assessment requests because all of the requests go through a centralized intelligence requirements group within the agency's engineering directorate.[25] This group has insight into the totality of the agency's threat assessment requests and is uniquely positioned to make determinations about the order of importance among them. As the group submits requests to the defense intelligence community, the defense intelligence community responds to the requests in the order that they were received, because, as we previously found, the defense intelligence community is not required to prioritize the requests, does not currently possess the

[24] GAO-07-388.

[25] MDA, Memorandum for All MDA Employees, *Missile Defense Agency Threat Baseline and Interaction with Intelligence, Counterintelligence and Law Enforcement Communities*, Policy Memorandum No. 67 (Fort Belvoir, Va.: Nov. 09, 2017).

capability to do so, and would not be in a position to dictate to an agency what is most important.[26]

Another opportunity for MDA to address the availability of threat assessments is through further collaboration with the defense intelligence community to determine the extent of additional resources that would be needed to enable accelerated support. When intelligence support requirements exceed the defense intelligence community's responsibilities, DOD acquisition programs are generally required to account for resources to augment intelligence support.[27] For example, according to defense intelligence community officials, the Air Force is providing one of the defense intelligence community's production centers with additional resources to collect data and devise tools primarily to support a specific major defense acquisition program via a military interdepartmental purchase request because the program's request exceeds the defense intelligence community's responsibilities.[28] According to MDA, intelligence mission data shortfalls are currently identified through an annual departmental review process. MDA stated that in fiscal year 2019 DOD approved budgeting additional funding in the future to help address intelligence mission data shortfalls for all of the military services, including MDA.

MDA has not provided the defense intelligence community with additional resources for an accelerated schedule to update threat modules more frequently. MDA has requested that the defense intelligence community update the digitized threat modules it needs to compile a BMDS VOLT report every year to ensure that it has the updated threat information needed for acquisition decisions; however, the defense intelligence community is only required to update the digitized threat modules every two years. Some defense intelligence community officials have acknowledged MDA's need to have an accelerated schedule, but have communicated to MDA that given its current manpower and resource

[26] GAO, *Defense Intelligence: Additional Steps Could Better Integrate Intelligence Input into DOD's Acquisition of Major Weapon Systems*, GAO-17-10 (Washington, D.C.: Nov. 1, 2016).

[27] Chairman of the Joint Chiefs of Staff Instruction 3170.01I, *Joint Capabilities Integration and Development System (JCIDS)* (Jan. 23, 2015); and JCIDS Manual Series, *Manual for the Operation of the Joint Capabilities Integration and Development System* (Feb. 12, 2015, including errata as of Dec. 18, 2015).

[28] The specific major defense acquisition program referenced in the example has been omitted due to classification.

constraints, the accelerated schedule is unrealistic without additional resources. Thus, MDA's request for the defense intelligence community to update the digitized threat modules faster exceeds what the defense intelligence community is currently able to do given its manpower and resource constraints.

With existing venues, like the VOLT Threat Steering Group, MDA and the defense intelligence community have a forum to further collaborate and identify what additional resources are needed and the potential funding scenarios to support an accelerated schedule for threat module production. Without collaboration through these existing venues, MDA and the defense intelligence community may not be utilizing an available method to ensure their individual needs are met. According to our best practices for inter-governmental agency collaboration, it is important for the inter-reliant agencies to collaboratively identify the resources—information, manpower, and funding—needed to accomplish their respective missions.[29] Doing so enables the agencies to have a common understanding and explore opportunities to leverage each other's resources; thus, realizing benefits that would not be available if they were working separately. Therefore, working together, MDA and the defense intelligence community would be better positioned to determine how to best meet their respective needs.

Opportunities Exist for MDA to Further Engage the Defense Intelligence Community on BMDS Acquisition to Address the Challenges of Keeping Pace with the Threat

MDA uses defense intelligence community threat assessments to inform its acquisitions, but the agency has not fully engaged the defense intelligence community on challenges in preparing the BMDS for existing and emerging threats. According to MDA, the rapid pace of threat evolution presents significant challenges for the agency to sufficiently plan for emerging threats. Although the defense intelligence community is uniquely positioned to assist MDA in addressing these challenges, the agency generally limits the defense intelligence community's insight into and input on critical threat-related BMDS acquisition processes and decisions, such as establishing the BMDS threat space and assigning threat parameters and threat models to BMDS elements. Major defense acquisition programs are generally required to engage the defense intelligence community on how to design and test weapon systems, but MDA generally does not, due to the acquisition flexibilities DOD has granted to the agency. Moreover, DIA is currently unable to validate

[29] GAO-06-15.

MDA's threat models, as required by DOD policy, because MDA does not follow the department's best practices on models and simulations. MDA has steadily increased its outreach to the defense intelligence community and other stakeholders over the past few years, but opportunities remain for more comprehensive engagement on key challenges the agency faces with keeping pace with the threat.

MDA Faces Challenges in Preparing the BMDS for Existing and Emerging Threats

According to MDA, the rapid pace of threat evolution presents significant challenges for the agency to sufficiently plan for emerging threats. MDA currently faces some difficult choices regarding what steps it needs to take and in what order to address recent threat advancements. In making these decisions, MDA has an opportunity to engage the defense intelligence community on whether and how it should make changes to the BMDS threat space, threat parameters, and threat models the agency uses as design requirements and test cases for BMDS elements. As previously noted, the defense intelligence community plays important stakeholder, advisor, and oversight roles for MDA's acquisitions. Although the department has provided MDA with flexibilities on following many of the requirements that specifically define when and how major defense acquisition programs are to engage the defense intelligence community, DOD policy requires MDA to vet its threat models and consult with the defense intelligence community on threat-related acquisition matters.[30]

DOD, senior defense officials, and expert panels supported by DOD have consistently maintained that the defense intelligence community's direct involvement in MDA's acquisitions is critical to staying ahead of the threat:

- In a written response following a 2002 congressional hearing, a senior defense official stated that every effort was being made to coordinate development of the document establishing the BMDS threat space with the defense intelligence community and that the defense

[30] DOD Instruction 5000.61, *DOD Modeling and Simulation (M&S) Verification, Validation, and Accreditation (VV&A)* (Dec. 9, 2009), p. 6; and DOD Directive 5134.09, *Missile Defense Agency (MDA)* (Sep. 17, 2009), p. 9-10.

intelligence community's participation was critical to the agency's success.[31]

- In 2010, DOD's Ballistic Missile Defense Review similarly found the need to maintain a strong focus by the defense intelligence community on the ballistic missile threat and that accurate and timely intelligence should play a vital role in informing BMDS planning.[32]
- In 2010, an expert panel known as JASON (not an acronym) found that MDA lacked sufficient plans for improving discrimination and that the agency risked falling behind the evolution of the threat's countermeasure capabilities.[33] The study recommended that DOD form stronger two-way connections between MDA and defense intelligence agencies.
- In 2012, the National Research Council found that MDA did not follow through on efforts to improve discrimination and that much of the agency's expertise on discrimination was lost in the late 2000s.[34] The study recommended that MDA seek assistance from experts with experience in understanding sensor data for threat missiles.
- In 2018, DOD's National Defense Strategy stated that modernizing missile defense, among other items, was necessary to keep pace with adversaries and that the department must expand the role of intelligence analysis throughout the acquisition process in order to streamline rapid, iterative approaches for delivering performance at what DOD refers to as "the speed of relevance."[35]
- During a 2018 congressional hearing, the Under Secretary of Defense for Research and Engineering stated that catching up to near-peer adversaries in missile defense can be achieved by exceeding their

[31] Pete Aldridge, Under Secretary of Defense for Acquisition, Technology, and Logistics, *Department of Defense Authorization for Appropriations for Fiscal Year 2003*, U.S. Senate, Committee on Armed Services, Subcommittee on Strategic Forces, 107th Congress (Washington, D.C.: Mar. 13, 2002).

[32] DOD, *Ballistic Missile Defense Review Report* (Washington, D.C.: Feb. 1, 2010).

[33] JASON, *MDA Discrimination*.

[34] National Research Council, *Making Sense of Ballistic Missile Defense*.

[35] DOD, *Summary of the 2018 National Defense Strategy of the United States of America: Sharpening the American Military's Competitive Edge* (Jan. 19, 2018).

technical capabilities and that the intelligence community was critical to making sure that we are outpacing our adversaries.[36]

MDA Limits the Defense Intelligence Community's Insight Into and Input on Some Critical Threat-Related BMDS Acquisition Processes and Decisions

Although MDA uses defense intelligence community threat assessments to inform BMDS acquisition, the defense intelligence community generally has limited insight into the BMDS, which is unprecedented among major defense acquisition programs. When MDA was established in 2002, DOD granted the agency exceptional flexibilities to diverge from the standard acquisition framework that most major defense acquisition programs follow. These flexibilities enable MDA to forego obtaining the defense intelligence community's input on some critical threat-related BMDS acquisition processes and decisions, such as how MDA establishes the:

- **threat space** that informs overall BMDS design and development;
- **threat parameters** assigned to each BMDS element as design requirements; and
- **threat models** assigned to each BMDS element as test cases for design reviews and testing.

However, according to MDA, the new BMDS VOLT report will serve as the source document for specific details on the BMDS threat space, threat parameters, and threat models.

Although MDA may leverage the defense intelligence community's threat assessments, MDA has not included the defense intelligence community in these key threat-related BMDS acquisition processes and decisions. For example, in response to a questionnaire we sent to MDA in May 2018, agency officials stated that decisions related to the threat parameters it assigns to the different BMDS elements should be left to MDA, as it is within the agency's purview and authority to design threats as it deems necessary for research, development, test, and evaluation purposes. Moreover, MDA indicated that the defense intelligence community should provide the agency with the best intelligence information on adversary missile capabilities, in a timely manner, to support the agency's mission. As such, MDA stated it does not support

[36] Dr. Michael Griffin, Under Secretary of Defense for Research and Engineering, *Hearing to Receive Testimony on Accelerating New Technologies to Meet Emerging Threats*, U.S. Senate, Committee on Armed Services, Subcommittee on Emerging Threats and Capabilities, 115th Congress (Washington, D.C.: Apr. 18, 2018).

obtaining the defense intelligence community’s concurrence on the threat parameters it assigns to the BMDS elements.

MDA has provided the defense intelligence community with some insight into the BMDS but not to the same extent DOD generally requires of major defense acquisition programs. For example, MDA has held a number of “immersion days” over the past nine years, which allow the defense intelligence community to receive briefings from MDA programs on priorities, future developments, and weapon system operations. According to MDA, it also assigns intelligence portfolio managers to BMDS elements and their mission, among other items, is to keep the defense intelligence community informed on key program developments and how intelligence feeds into the agency’s threat-related acquisition processes and decisions. In addition, MDA has briefed the DIBMAC on how it uses threat assessments to inform BMDS acquisition. However, defense intelligence community officials stated that they generally lack fundamental information on the BMDS and have no visibility into the BMDS threat space, threat parameters, or test cases MDA assigns to the BMDS elements.

In contrast, for most major defense acquisition programs, the defense intelligence community is integrally involved in determining the:

- threat(s) of record upon which requirements of the weapon system are based;
- key performance parameters and attributes of the weapon system;
- threat parameters that could critically degrade or negate the weapon system; and
- operational threat environment the weapon system is tested against.

These insights, enabled by DOD’s standard requirements-setting process and acquisition framework, are intended to provide the defense intelligence community with in-depth knowledge of the design and performance requirements for most major DOD weapon systems.

Officials from other various organizations we met with, such as the Joint Staff, contractors, warfighters, and test and evaluation, expressed concerns about MDA’s ability to unilaterally define the threats it designs the BMDS against. As one MDA prime contractor told us, what really matters is how the BMDS would perform in the real world against real threats. Defense intelligence community officials acknowledged that MDA, as the BMDS developer, has a legitimate need to explore threat capabilities beyond those that the intelligence community has observed from specific adversaries. However, defense intelligence community officials rejected a sentiment expressed to us by MDA officials that the defense intelligence community lacks expertise in understanding the bounds of threat capabilities. To the contrary, according to defense intelligence community officials, this is exactly the type of analysis at which the defense intelligence community excels. In choosing not to engage the defense intelligence community on these key threat-related BMDS acquisition processes and decisions, MDA runs the risk of not sufficiently planning for existing and emerging threats.

MDA's reluctance to provide the defense intelligence community with insight into or input on some threat-related BMDS acquisition processes and decisions is consistent with how MDA has engaged other DOD stakeholders and oversight groups. Our prior work on defense acquisitions has shown that establishing buy-in from decision makers is a key enabler of achieving better acquisition outcomes because DOD components provide varying perspectives due to their unique areas of expertise and experience.[37] However, in May 2017, we found that MDA generally limits the warfighter's input on the requirements it pursues and overlooked stakeholder concerns on the acquisition strategy for a redesigned kill vehicle for the Ground-based Midcourse Defense system.[38] We made recommendations aimed at increasing stakeholder engagement and oversight in BMDS acquisition, such as coordinating operational requirements with the warfighter and obtaining input from DOD's Office for Cost Assessment and Program Evaluation (CAPE) on acquisition strategies for new efforts. DOD's acting Assistant Secretary of Defense (Acquisitions) did not concur with the recommendations, stating that warfighters lacked the skillset to determine operational BMDS requirements and existing DOD policy does not require MDA to obtain CAPE's concurrence on acquisition policies. We continue to maintain that DOD should implement the recommendations.

[37] GAO, *Missile Defense: Some Progress Delivering Capabilities, but Challenges with Testing Transparency and Requirements Development Need to Be Addressed*, GAO-17-381 (Washington, D.C.: May 30, 2017).

[38] GAO-17-381.

DIA Is Currently Unable to Validate MDA's Threat Models, as Generally Required by DOD Policy

MDA builds its own threat models to support BMDS design, development, and testing but it does not validate its threat models with DIA, which is inconsistent with DOD policy and best practices. Although the defense intelligence community builds threat models, MDA cannot currently use those models as-is because they are generally not compatible with MDA's modeling and simulation framework.[39] Even with MDA using its own threat models, DOT&E has found that integrating the various BMDS models and presenting them with a common threat scene has been an extremely challenging task for MDA.[40] Moreover, MDA's BMDS modeling and simulation architecture requires highly detailed threat models for simulations to function properly. Defense intelligence community officials stated that they generally do not need the same level of detail MDA requires for the types of analyses the defense intelligence community performs. In addition, according to a March 2018 MDA memorandum, the agency was previously told by representatives of the DIBMAC that they do not have the staff or resources to produce the high volumes of detailed threat models that MDA needs to support BMDS development and testing.[41] Therefore, MDA continues to build its own threat models for use in BMDS development and testing.

MDA uses defense intelligence community threat assessments to build its threat models, but independent evaluators have not been able to fully trace MDA's threat models to defense intelligence community threat assessments. According to a briefing MDA presented to the defense intelligence community in September 2018, every target, model, and test can be traced back to defense intelligence data. However, in August 2018, the U.S. Army issued a memorandum for MDA stating that the BMDS Operational Test Agency (OTA)—the agency responsible for independently analyzing the verification and validation data for models used in operational testing—was only able to certify some of the threat models used in a recent ground test.[42] In other ground tests, though, the BMDS OTA was able to trace MDA's threat models back to defense

[39] Each of the BMDS elements maintains its own set of models and simulations, which MDA brings together at the BMDS-level as a federated framework.

[40] DOT&E, *2017 Assessment of the BMDS*.

[41] MDA, *Memorandum for Director, Defense Intelligence Agency: Requested Validated Intelligence to Meet GAO Mandate Audit Finding on Intelligence Support to Ballistic Missile Defense System Development and Testing* (Ft. Belvoir, VA.: Mar. 5, 2018).

[42] The precise number of models certified by the BMDS OTA has been omitted because it is classified.

intelligence community threat assessments. In February 2019, DOT&E reported that (a) credible threat models are the linchpins of BMDS models and simulation; (b) reducing threat model uncertainty is a high priority; and (c) MDA and the BMDS OTA should ensure that MDA-developed threat models are representative of the defense intelligence community's understanding of the threat.[43]

MDA also has not implemented best practices established by DOD's Models and Simulation Coordination Office that would enable DIA to be in a position to validate MDA's threat models. According to DOD best practices on modeling and simulation, the validation agent should: (1) be brought on in the beginning of the modeling and simulation development process; (2) work closely with the model developers as the models are built and tested; and (3) perform validation as a continuing activity of the overall process of developing and preparing a model for use or reuse in a simulation.[44] Conversely, defense intelligence community officials stated that they lack sufficient insight into and input on how MDA builds and uses threat models. For example, the defense intelligence community has emphasized to MDA that caveats need to be carried through with the model data and voiced concerns about the engineering judgments the agency makes in its threat models, because these judgments could lead to the BMDS performing well or poorly for reasons not based on the actual threat. Given these uncertainties and the defense intelligence community's lack of insight into the purposes for which MDA uses its threat models, DIA lacks the insight and input necessary to validate MDA's threat models.

Although MDA has previously expressed interest in validating its threat models with the defense intelligence community, long-standing obstacles remain. During a May 2018 meeting between MDA and the DIBMAC, defense intelligence community officials identified the lessons they have learned from working with other acquisition programs to validate threat models. Model validation can be achieved if the acquisition program:

- establishes a partnership with the defense intelligence community;

[43] DOT&E, *2018 Assessment of the Ballistic Missile Defense System*, Feb. 2019.

[44] DOD Models and Simulation Coordination Office, *Models and Simulations Verification, Validation, and Accreditation Recommended Practices Guide*, "Introduction" and "V&V Agent's Role in W&A of New Development," accessed Feb. 14, 2019, https://vva.msco.mil.

- prioritizes its threat modeling needs;
- recognizes there are limits to how many threat models can be built in a given time;
- provides in-depth insight into its threat modeling needs and weapon system's capabilities;
- discusses how the models will be applied;
- jointly defines model acceptance criteria early in the process;
- provides resources, including funding and staff; and
- invests in the defense intelligence community's capability and capacity.

MDA officials stated that the agency desires to have its threat models validated but noted that the defense intelligence community does not validate models produced by other organizations. MDA officials also emphasized that the defense intelligence community cannot meet MDA's timeline for building threat models, whereas the agency can. In addition, MDA officials indicated to us that they do not believe it is practical to provide the amount of insight defense intelligence community officials told us they would need in order to validate MDA's threat models. MDA officials told us that the only way in which the defense intelligence community could obtain such insight is by being co-located with MDA's threat modelers as the models are being built. However, the 2010 JASON study found that this type of close working arrangement between MDA engineers and defense intelligence analysts is necessary to effectively plan for emerging threats. Defense intelligence community officials also clarified for MDA that the defense intelligence community can validate models produced by another agency but it would require the defense intelligence community having detailed knowledge of everything used to produce the model.

As a result, although DOD policy generally requires that threat models used to support acquisition decisions be validated by DIA, MDA has yet to validate any of the numerous threat models it has developed since 2004.[45] Without independent validation, MDA runs the risk that DOD and congressional decisionmakers may not have confidence that the agency's

[45] Both the current version of DOD Instruction 5000.61 (issued December 9, 2009) and the prior version (issued May 13, 2003) designated the DIA Director as the validation authority for representations of non-U.S. forces and capabilities and other DOD components' representations of foreign forces, respectively.

plans and proposals for developing the BMDS are appropriate and sufficient to address the threat because any flaws or bias in MDA's threat models can have significant implications on the BMDS's overall performance. According to a Federally Funded Research and Development Center publication describing its efforts supporting MDA threat modeling, acquisition influences can place pressure on MDA threat modelers to tailor the missile threats to suit the currently feasible BMDS design.[46] In May 2017, we found a parallel circumstance where, in the absence of warfighter validation of MDA-established requirements, the agency made critical design choices for three new BMDS efforts.[47] These design choices reflected the needs and preferences of MDA ahead of the warfighter, potentially compromising performance to the extent of not being able to defeat current and future threats.

MDA Has Steadily Increased Its Outreach to DOD Stakeholders Over the Past Few Years, but Opportunities Remain for Further Engagement

MDA has undertaken a number of efforts over the past few years to generally increase stakeholder involvement in BMDS acquisition. The engagement efforts, in large part, are a result of efforts led by MDA's previous director to improve the agency's relationship with department stakeholders.[48] In addition to previously serving as the Deputy Director for MDA, the Director also held a variety of assignments in operational, acquisition, and staff units within DOD. When we met with the MDA Director in March 2018, he told us that he wanted to change the agency's culture of limiting stakeholder input, noting that he had recently provided updated guidance to his leadership team and agency personnel on bringing stakeholders in early, engaging them more frequently and substantively, and ensuring that the agency has obtained their buy-in on major undertakings. The MDA Director also stated that he was willing to take some actions that could effectively address a recommendation we made in May 2017 intended to provide the warfighter with greater input on

[46] The Aerospace Corporation, "Ballistic Missile Threat Modeling," *Crosslink,* Vol. 9, No. 1 (Los Angeles, CA: Spring 2008).

[47] GAO-17-381.

[48] In May 2019, a new MDA Director took over as head of the agency.

operational requirements for ballistic missile defense.[49] Officials from several DOD organizations we met with over the course of our review observed that MDA's engagement with their respective organizations was improving.

In 2018, MDA began working with the defense intelligence community to determine a more appropriate level of involvement for the defense intelligence community throughout MDA's acquisition activities. MDA and defense intelligence community officials agreed during a May 2018 meeting that processes could be put in place to develop intelligence-based countermeasure assessments if adequate resources are provided. MDA officials also acknowledged that the defense intelligence community would benefit from having a better understanding of how the BMDS responds to threats and agreed to work towards providing such information. Defense intelligence community officials stated that increased insight would allow them to better focus their intelligence collection, analysis, and production by knowing which threat parameters MDA most often uses and the specificity of those parameters. The defense intelligence community and MDA also agreed that providing defense intelligence community engineers with MDA program-level access would improve the support the defense intelligence community provides to MDA.

MDA has also recently increased its outreach to the defense intelligence community on some early BMDS planning decisions, although opportunities for more comprehensive engagement remain. For example, MDA engaged the defense intelligence community on an analysis of alternatives the agency completed in February 2017 that assessed future sensor options for the BMDS. According to MDA officials, they are also engaging the defense intelligence community on another analysis of alternatives pertaining to defense against hypersonic missiles. In addition,

[49] In May 2017, we recommended that DOD transition responsibility of setting operational-level requirements for missile defense to the warfighter and, in the interim, require MDA to coordinate a key requirements document, called the Achievable Capabilities List (ACL), with the warfighter (see GAO-17-381). During a meeting with the MDA Director in March 2018, the Director agreed to coordinate the ACL with the warfighter and was amenable to more in-depth warfighter input on operational needs, provided those needs are approved by the Combatant Commander for U.S. Strategic Command and communicated via a warfighter needs document called the Prioritized Capabilities List (PCL). In October 2018, warfighters from U.S. Strategic Command's Joint Functional Component Command for Integrated Missile Defense confirmed that MDA was coordinating the ACL with them and a tentative agreement was reached with MDA for the warfighter to provide greater definition of its operationally needed capabilities in the PCL.

MDA worked with the defense intelligence community to establish threat space parameters for some specific threat systems.[50] Also, as noted earlier, over the last nine years, MDA has held 18 “immersion day” events with the defense intelligence community, half of which occurred in the last two years. Moving forward, MDA has opportunities to more comprehensively engage the defense intelligence community on updating the BMDS threat space and determining threat parameters and threat models assigned as design requirements and test cases for BMDS elements.

In addition, MDA has recently begun placing greater emphasis on ensuring its models are credible. According to an internal MDA memorandum signed by the MDA Director in April 2018, a culture exists within the agency that generally tolerates the use of models that have not been sufficiently vetted and is too willing to accept the associated risk.[51] The memorandum states that the agency’s goal is for all MDA personnel to help address this culture problem and that model verification, validation, and accreditation is a high priority for MDA. During a meeting with the BMDS OTA in October 2018, officials confirmed that MDA is taking steps to address the challenges raised in the memorandum.

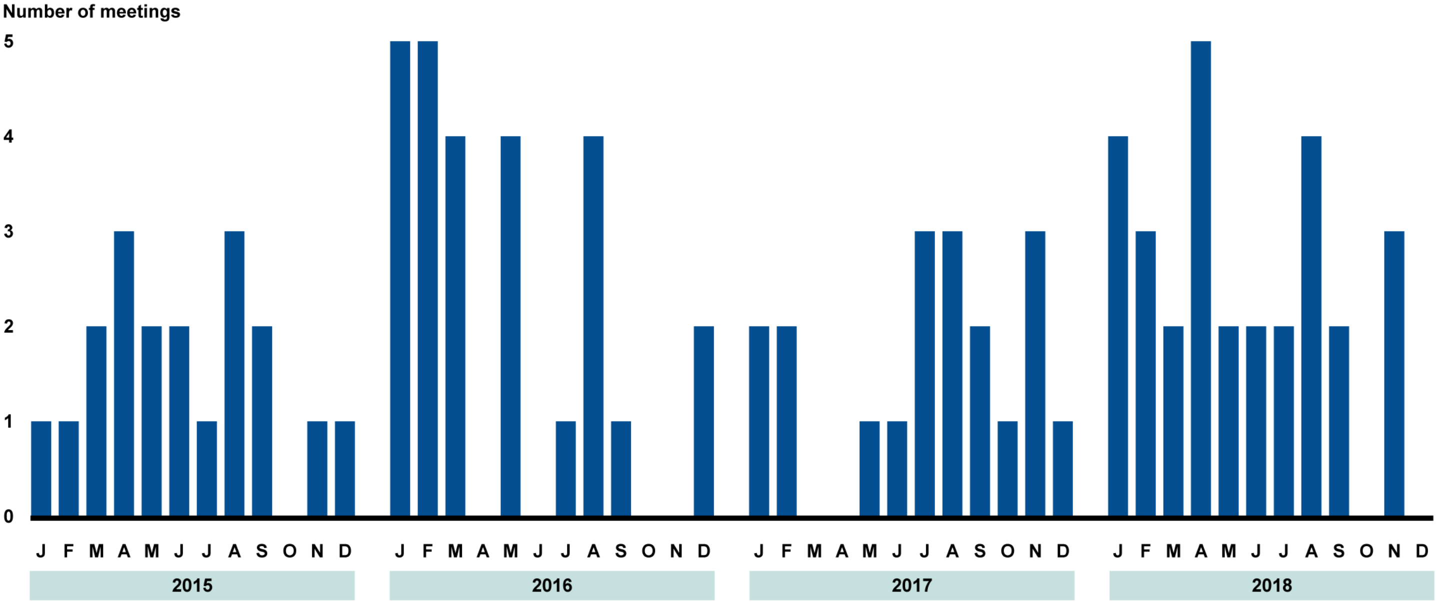
MDA also increased its outreach to the defense intelligence community in 2016 to coordinate on threat modeling efforts. In the past three years, MDA and the defense intelligence community have collaborated to quickly model several newly-observed threat missiles, according to MDA.[52] Figure 6 below shows that MDA held 93 threat model coordination meetings with the defense intelligence community over the last four years, with more frequent meetings occurring in early 2016 and again in early-to-mid 2018. In addition, MDA is working with the defense intelligence community to address compatibility issues that currently prevent MDA from directly using the defense intelligence community’s threat models in BMDS ground testing. MDA plans to include a few missile trajectory models produced by the defense intelligence community in the models and simulation framework for the agency’s upcoming Ground Test-08 campaign.

[50] Some specific information related to the examples cited has been omitted because it is classified.

[51] MDA, Memorandum for All MDA, *Accredited Models and Simulations for Ballistic Missile Defense System Assessment* (Fort Belvoir, VA: Apr. 02, 2018).

[52] The specific threat missiles have been omitted due to classification.

Figure 6: Meetings between Missile Defense Agency (MDA) and the Defense Intelligence Community to Coordinate on Threat Modeling Efforts, January 2015 - December 2018



Source: GAO analysis of MDA and intelligence community data. | GAO-20-177

The Technical Interchange Meetings and pathfinder efforts for MDA directly using defense intelligence community threat models are improving collaboration between MDA and the defense intelligence community on threat modeling efforts. However, they do not provide MDA with a pathway for validating its threat models with DIA. Even if compatibility issues that currently prevent MDA from using defense intelligence community threat models could be resolved, the defense intelligence community is currently not resourced to build threat models for MDA. Moreover, although MDA has indicated that the Technical Interchange Meetings can include any topic of interest, the meetings do not provide defense intelligence officials with sufficient insight into how MDA builds its models, including the assumptions, caveats, or intended use of the models.

According to MDA, the agency continues to hold discussions with the defense intelligence community and explore process improvements, as well as technical and resource requirements, to ensure the creation of valid, threat-representative models for BMDS development. In March 2018, the MDA Director told us that one of his priorities was to ensure that the agency was using appropriately validated models and acknowledged the importance of ensuring its threat models are sufficiently representative. In April 2018, MDA subsequently began holding meetings with the DIBMAC to define the issues preventing the defense intelligence community from validating MDA's threat models. MDA and the defense intelligence community met five times in 2018 to identify actions that would facilitate working together to develop threat models the defense intelligence community would be comfortable validating. During these meetings, both organizations agreed on specific actions intended to increase the defense intelligence community's involvement in MDA's threat modeling process. To achieve threat model validation, an initial plan was developed that included a combination of (a) MDA directly using aspects of defense intelligence community threat models; and (b) MDA partnering with the defense intelligence community to build threat models. MDA and the defense intelligence community plan to hold follow-on meetings in 2019 to further discuss the plan and review actions.

Conclusions

MDA is reliant on threat assessments from the defense intelligence community, as they inform what weapon systems the agency pursues, the design of those systems, and how those systems are tested prior to being delivered to the warfighter for operational use. However, the defense intelligence community has been facing a variety of challenges that are affecting its ability to provide MDA the threat assessments it needs, when it needs them. If MDA does not have the threat assessments it needs, when needed, the agency's weapon systems are at risk of being designed or tested against irrelevant or outdated information, which could result in performance shortfalls and costly retrofits. MDA has opportunities to mitigate these challenges and risks by collectively prioritizing its threat assessment requests and working through existing venues with the intelligence community to determine if and to what extent additional resources may be needed to secure the support that it needs. If MDA does not take advantage of these opportunities, the defense intelligence community's challenges will likely continue, which will impact the availability of threat assessments and increase the likelihood that MDA's weapon systems will not be designed or tested against the most up-to-date threat information.

In addition, MDA faces a steep challenge in developing the BMDS and fielding capabilities at a rate that keeps pace with the threat. MDA was previously informed by expert panels and senior defense leaders that it needed to work more closely with the defense intelligence community to better prepare for future threats or risk falling behind the threat. Given these challenges, it is imperative for MDA to make the most out of its available resources. Aside from providing MDA with threat assessments, the defense intelligence community is a resource MDA has yet to fully tap into. The defense intelligence community is uniquely qualified to assist MDA on fundamental and critically important BMDS acquisition processes and decisions, such as establishing the BMDS threat space and the threat parameters and models it assigns to the BMDS elements. Moreover, after nearly 15 years of building numerous threat models, MDA has yet to fully implement a plan for DIA to validate these threat models, as generally required by DOD policy. However, MDA has recently begun laying the groundwork for more comprehensive engagement with the defense intelligence community through efforts which have the potential to address long-standing obstacles that have prevented DIA from validating MDA's threat models. Resolving these issues would help MDA keep pace with emerging threats and improve the BMDS's viability to defend against the complex missile threats of the future.

Recommendations for Executive Action

We are making a total of three recommendations to DOD:

The Director, MDA should coordinate with the defense intelligence community on the agency's collective priorities for threat assessments and work with the defense intelligence community to determine if additional resources are needed to support the agency's threat assessment needs. (Recommendation 1)

The Director, MDA should fully engage the defense intelligence community on key threat-related missile defense acquisition processes and decisions, including providing insight into and obtaining input from the defense intelligence community on the threat space MDA establishes for the BMDS and the threat parameters and threat models MDA assigns to BMDS elements as design requirements and test cases. (Recommendation 2)

The Secretary of Defense should require the Director, MDA and the Director, DIA to coordinate on establishing a process for MDA to obtain validation of its threat models. (Recommendation 3)

Agency Comments and Our Evaluation

DOD provided written comments in response to the classified version of this report (GAO-19-92C), indicating that the department concurred with all three of our recommendations. An edited version of DOD's comments is reprinted in appendix II as some information had to be omitted due to classification. In addition, the summarized version of DOD's comments below is reflective of the content in the classified version. DOD provided us with technical comments and a significant amount of new information in response to the classified version of this report. We incorporated this information into our report, as appropriate, but the new information did not substantively change our findings and did not alter our recommendations. Although DOD concurred with our third recommendation, DOD also raised concerns about statements in our report related to our third recommendation that the department believes are inaccurate. We do not believe DOD's concerns are warranted because our findings are based on evidence we obtained during our review—evidence that we believe is sufficient and appropriate and provides a reasonable basis for our findings and conclusions. We address this in further detail below.

DOD concurred with our first recommendation that the Director, MDA should coordinate with the defense intelligence community on the agency's collective priorities for threat assessments and determine whether additional resources are needed. In its response, DOD stated that MDA will continue to follow established processes to identify threat assessment needs and to determine if additional resources are required. However, our review found that these established processes—prioritizing exclusively through distinct, individual threat assessment lanes—have not proven entirely effective. In addition, although MDA has participated in the department's intelligence mission data review process since 2016, the agency has yet to provide the defense intelligence community with additional resources to address known funding and manpower shortages. Moreover, this review process is limited to intelligence mission data and does not cover all of the other types of threat assessments that MDA needs. As such, we maintain that MDA should take additional steps beyond continuing existing processes to address the challenges MDA currently faces in obtaining the threat assessments it needs, when it needs them.

DOD also concurred with our second recommendation that the Director, MDA should provide insight into and obtain input from the defense intelligence community on the threat space MDA establishes for the BMDS and the threat parameters and threat models the agency assigns to BMDS elements as design requirements and test cases. DOD stated in its response that MDA has and will continue to fully engage the defense intelligence community on key threat-related missile defense acquisition processes and decisions. The efforts MDA has recently undertaken to expand its outreach to the defense intelligence community are positive steps. However, we have yet to see MDA provide the defense intelligence community with further insight into or input on the threat space the agency has established for the BMDS or the assignment of threat models and threat parameters to BMDS elements. We will continue to monitor MDA's ongoing efforts to see whether it takes this next step toward more fully engaging the defense intelligence community.

DOD concurred with our third recommendation that the Secretary of Defense should require the MDA and DIA Directors to coordinate on establishing a process for MDA to obtain validation of its threat models. In its response, DOD stated that the department will re-examine the most cost-effective approach to meet the intent of DIA validation to support development and fielding of effective BMDS elements. More specifically, DOD stated that MDA and the DIBMAC are currently having extensive discussions regarding how the defense intelligence community can best support MDA's threat modeling requirements. As noted in our report, the discussions MDA has had with the defense intelligence community over the course of 2018 demonstrate that the department is beginning to consider substantive measures to address the long-standing issue of MDA not using DIA-validated threat models. However, MDA and defense intelligence community officials have also cautioned that obstacles remain and that alternative solutions may need to be explored. We will continue to monitor these ongoing discussions and any results that emerge.

DOD also stated in its response that it was concerned that statements in our report pertaining to our third recommendation imply that MDA has not coordinated with DIA on validating its threat models and that our report could be interpreted as saying MDA does not internally conduct threat model validation. To be clear, our review did, in fact, find that, until recently, MDA did not sufficiently coordinate with DIA on establishing a process for creating valid threat models for use in MDA simulations. Furthermore, we explain in our report that MDA was told that the defense intelligence community can validate MDA's threat models if it has sufficient insight into how MDA builds its models—insight which MDA officials previously told us was unnecessary. Additionally, although MDA may internally validate its threat models for each ground test, the BMDS OTA was not able to certify many of those threat models, in part, because some models could not be traced back to the defense intelligence community's threat assessments. We therefore excluded MDA's internal threat model validation process from our report, as it is not a comparable substitute for DIA threat model validation.

We are sending copies of this report to the appropriate congressional committees and the Secretary of Defense. In addition, the report is available at no charge on the GAO website at http://www.gao.gov.

If you or your staff have any questions about this report, please contact me at (202) 512-4841 or chaplainc@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this report. GAO staff who made key contributions to this report are listed in appendix III.

Cristina T. Chaplain
Director, Contracting and National Security Acquisitions

List of Committees

The Honorable James M. Inhofe
Chairman
The Honorable Jack Reed
Ranking Member
Committee on Armed Services
United States Senate

The Honorable Richard Shelby
Chairman
The Honorable Richard Durbin
Ranking Member
Subcommittee on Defense
Committee on Appropriations
United States Senate

The Honorable Adam Smith
Chairman
The Honorable Mac Thornberry
Ranking Member
Committee on Armed Services
House of Representatives

The Honorable Pete Visclosky
Chairman
The Honorable Ken Calvert
Ranking Member
Subcommittee on Defense
Committee on Appropriations
House of Representatives

Appendix I: Defense Intelligence Components Responsible for Assessing Foreign Ballistic Missiles

In its entirety, the intelligence community is a federation of 17 agencies and organizations that span the executive branch of the U.S. government. The defense intelligence components responsible for assessing foreign ballistic missile threats are headed by the Defense Intelligence Agency and overseen and coordinated by the Defense Intelligence Ballistic Missile Analysis Committee. Table 4 below identifies each component and its respective focus areas.

Table 4: Defense Intelligence Community Components Responsible for Assessing Foreign Ballistic Missile Threats

Defense intelligence component	Assesses
Defense Intelligence Agency, Missile and Space Intelligence Center	The technical characteristics, capabilities, performance, limitations, effectiveness, and vulnerabilities of current, developmental, and projected short-range[a] and certain close-range[b] foreign ballistic missile systems.
Defense Intelligence Agency, Defense Technology and Long-Range Analysis Office	Long-range projections of forces, in order to develop and manage a future order of battle based on these projections.
Defense Intelligence Agency, Regional Centers	Strategy and doctrine at the national and operational levels of the military command structure, organizational and modernization plans for future enhancements of national ballistic missile forces, and the order of battle for missile forces, including status, organization, and equipment.
U.S. Air Force, National Air and Space Intelligence Center	The technical characteristics, capabilities, performance, limitations, effectiveness, and vulnerabilities of long-range[c] ballistic missile systems, which include medium-, intermediate-, and intercontinental-range missiles.
U.S. Navy, Office of Naval Intelligence	Submarine and ship-launched naval ballistic missile systems and vulnerabilities, including vulnerabilities to offensive cyber operations.
U.S. Army, National Ground Intelligence Center	The technical characteristics, capabilities, performance, limitations, effectiveness, and vulnerabilities of ballistic missile transporters and launchers, as well as the technical characteristics of certain current, developmental, and projected close-range foreign ballistic missile systems.

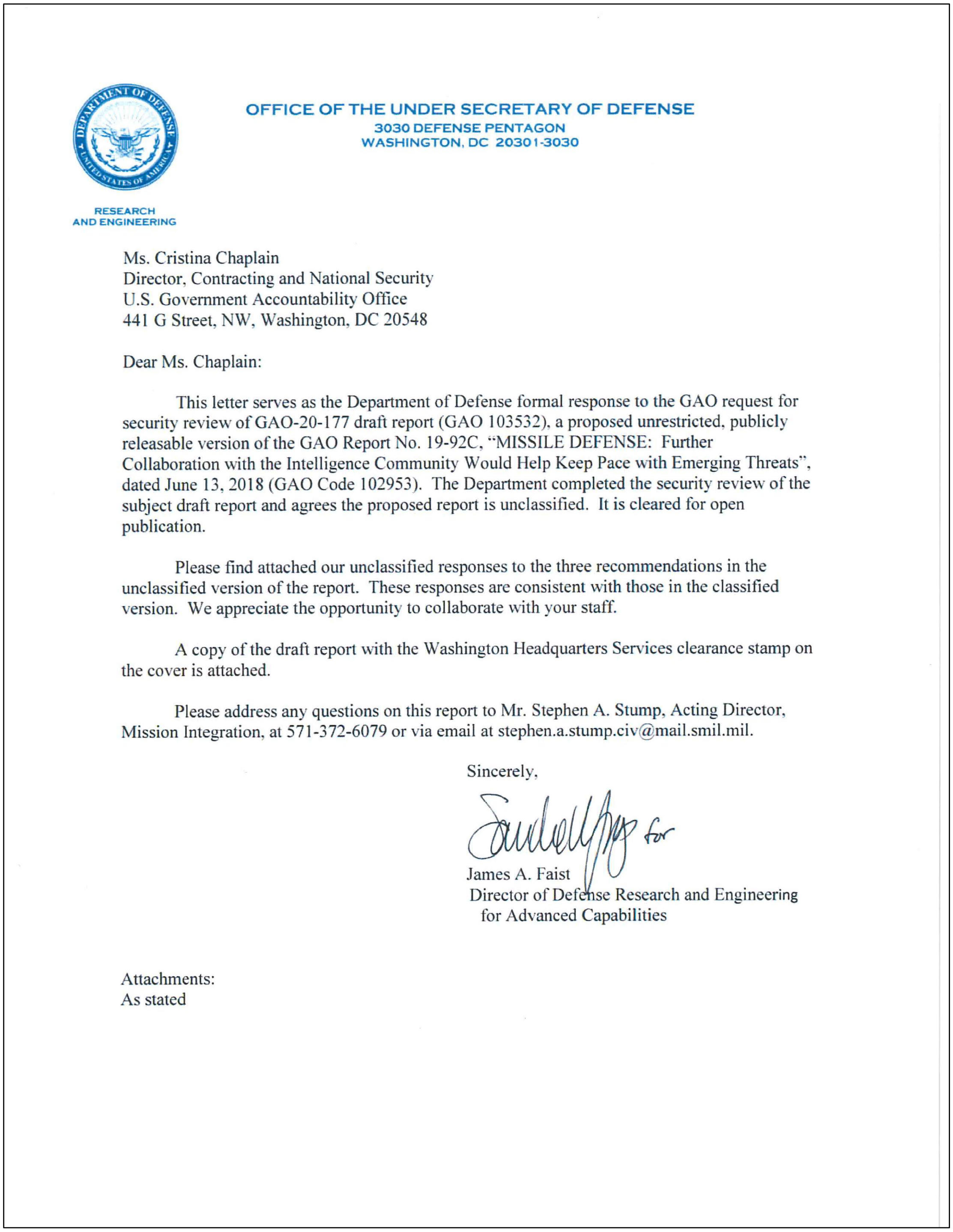
Source: GAO summary of DOD information. | GAO-20-177

[a] Short-range ballistic missiles have a range of 300-1,000 kilometers.

[b] Close-range ballistic missiles have a range of 50-300 kilometers.

[c] Long-range ballistic missiles have a range greater than 1,000 kilometers.

Appendix II: Comments from the Department of Defense



OFFICE OF THE UNDER SECRETARY OF DEFENSE
3030 DEFENSE PENTAGON
WASHINGTON, DC 20301-3030

RESEARCH
AND ENGINEERING

Ms. Cristina Chaplain
Director, Contracting and National Security
U.S. Government Accountability Office
441 G Street, NW, Washington, DC 20548

Dear Ms. Chaplain:

This letter serves as the Department of Defense formal response to the GAO request for security review of GAO-20-177 draft report (GAO 103532), a proposed unrestricted, publicly releasable version of the GAO Report No. 19-92C, "MISSILE DEFENSE: Further Collaboration with the Intelligence Community Would Help Keep Pace with Emerging Threats", dated June 13, 2018 (GAO Code 102953). The Department completed the security review of the subject draft report and agrees the proposed report is unclassified. It is cleared for open publication.

Please find attached our unclassified responses to the three recommendations in the unclassified version of the report. These responses are consistent with those in the classified version. We appreciate the opportunity to collaborate with your staff.

A copy of the draft report with the Washington Headquarters Services clearance stamp on the cover is attached.

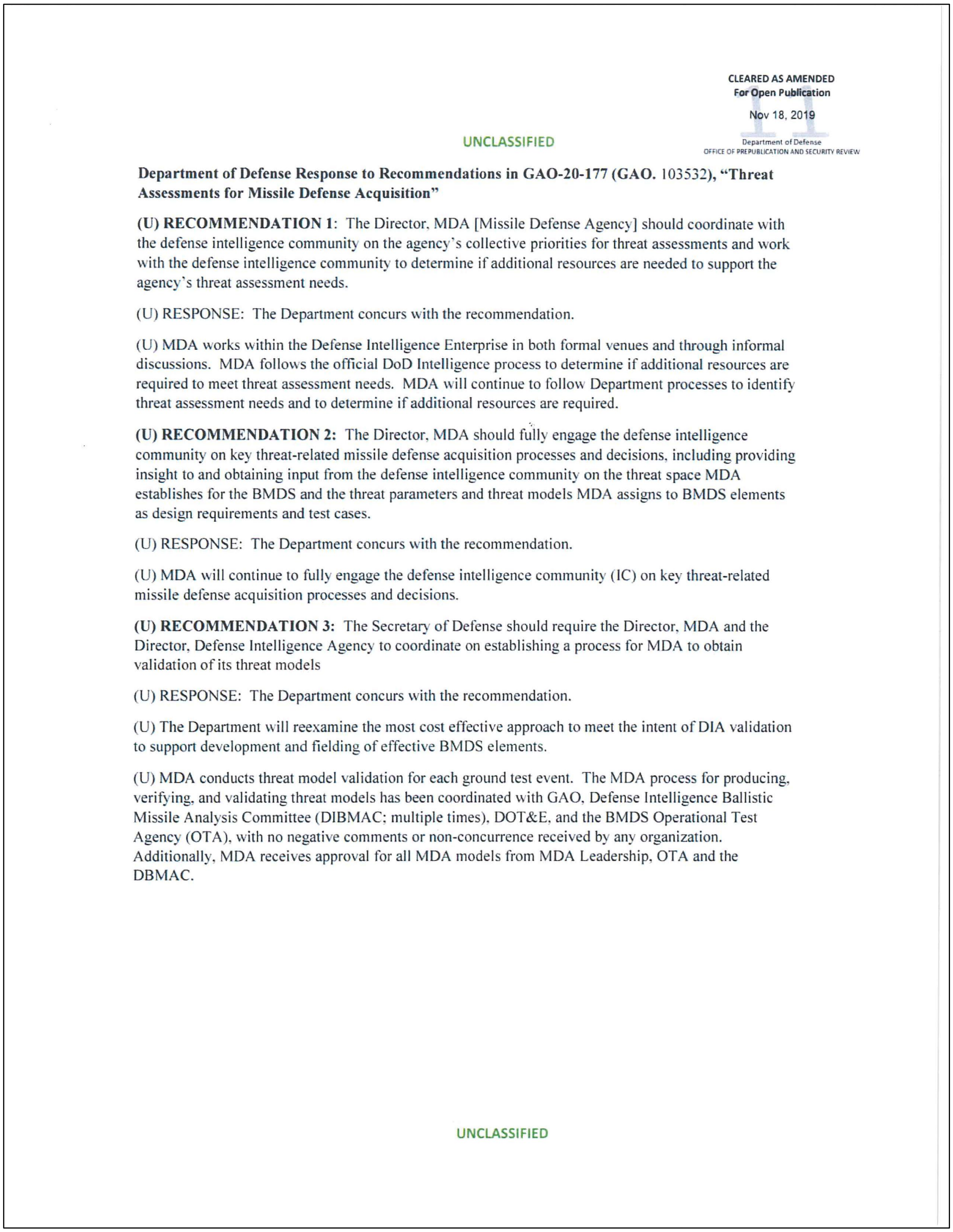
Please address any questions on this report to Mr. Stephen A. Stump, Acting Director, Mission Integration, at 571-372-6079 or via email at stephen.a.stump.civ@mail.smil.mil.

Sincerely,

for

James A. Faist
Director of Defense Research and Engineering
for Advanced Capabilities

Attachments:
As stated



UNCLASSIFIED

Department of Defense Response to Recommendations in GAO-20-177 (GAO. 103532), "Threat Assessments for Missile Defense Acquisition"

(U) RECOMMENDATION 1: The Director, MDA [Missile Defense Agency] should coordinate with the defense intelligence community on the agency's collective priorities for threat assessments and work with the defense intelligence community to determine if additional resources are needed to support the agency's threat assessment needs.

(U) RESPONSE: The Department concurs with the recommendation.

(U) MDA works within the Defense Intelligence Enterprise in both formal venues and through informal discussions. MDA follows the official DoD Intelligence process to determine if additional resources are required to meet threat assessment needs. MDA will continue to follow Department processes to identify threat assessment needs and to determine if additional resources are required.

(U) RECOMMENDATION 2: The Director, MDA should fully engage the defense intelligence community on key threat-related missile defense acquisition processes and decisions, including providing insight to and obtaining input from the defense intelligence community on the threat space MDA establishes for the BMDS and the threat parameters and threat models MDA assigns to BMDS elements as design requirements and test cases.

(U) RESPONSE: The Department concurs with the recommendation.

(U) MDA will continue to fully engage the defense intelligence community (IC) on key threat-related missile defense acquisition processes and decisions.

(U) RECOMMENDATION 3: The Secretary of Defense should require the Director, MDA and the Director, Defense Intelligence Agency to coordinate on establishing a process for MDA to obtain validation of its threat models

(U) RESPONSE: The Department concurs with the recommendation.

(U) The Department will reexamine the most cost effective approach to meet the intent of DIA validation to support development and fielding of effective BMDS elements.

(U) MDA conducts threat model validation for each ground test event. The MDA process for producing, verifying, and validating threat models has been coordinated with GAO, Defense Intelligence Ballistic Missile Analysis Committee (DIBMAC; multiple times), DOT&E, and the BMDS Operational Test Agency (OTA), with no negative comments or non-concurrence received by any organization. Additionally, MDA receives approval for all MDA models from MDA Leadership, OTA and the DBMAC.

UNCLASSIFIED

Appendix III: GAO Contact and Staff Acknowledgments

GAO Contact

Cristina Chaplain at (202)512-4841 or chaplainc@gao.gov

Staff Acknowledgements

In addition to the contact named above, LaTonya Miller (Assistant Director), Rose Brister, Lori Fields, Laura Greifner, Kurt Gurka, Helena Johnson, Kevin O'Neill, Jay Tallon, Brian Tittle, Hai Tran, Alyssa Weir, and Robin Wilson made key contributions to this report.

(103532)

GAO's Mission

The Government Accountability Office, the audit, evaluation, and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through our website. Each weekday afternoon, GAO posts on its website newly released reports, testimony, and correspondence. You can also subscribe to GAO's email updates to receive notification of newly posted products.

Order by Phone

The price of each GAO publication reflects GAO's actual cost of production and distribution and depends on the number of pages in the publication and whether the publication is printed in color or black and white. Pricing and ordering information is posted on GAO's website, https://www.gao.gov/ordering.htm.

Place orders by calling (202) 512-6000, toll free (866) 801-7077, or
TDD (202) 512-2537.

Orders may be paid for using American Express, Discover Card, MasterCard, Visa, check, or money order. Call for additional information.

Connect with GAO

Connect with GAO on Facebook, Flickr, Twitter, and YouTube.
Subscribe to our RSS Feeds or Email Updates. Listen to our Podcasts.
Visit GAO on the web at https://www.gao.gov.

To Report Fraud, Waste, and Abuse in Federal Programs

Contact FraudNet:

Website: https://www.gao.gov/fraudnet/fraudnet.htm

Automated answering system: (800) 424-5454 or (202) 512-7700

Congressional Relations

Orice Williams Brown, Managing Director, WilliamsO@gao.gov, (202) 512-4400,
U.S. Government Accountability Office, 441 G Street NW, Room 7125,
Washington, DC 20548

Public Affairs

Chuck Young, Managing Director, youngc1@gao.gov, (202) 512-4800
U.S. Government Accountability Office, 441 G Street NW, Room 7149
Washington, DC 20548

Strategic Planning and External Liaison

James-Christian Blockwood, Managing Director, spel@gao.gov, (202) 512-4707
U.S. Government Accountability Office, 441 G Street NW, Room 7814,
Washington, DC 20548