

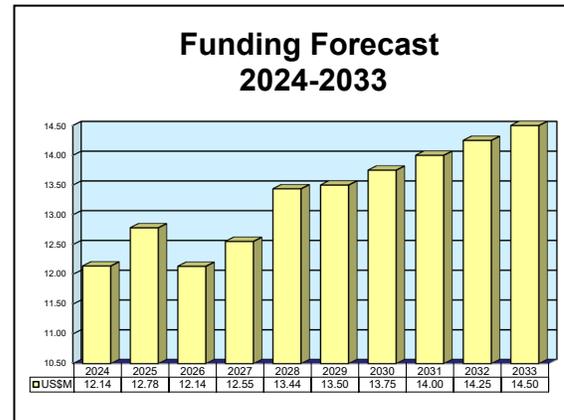
ARCHIVED REPORT

For data and forecasts on current programs please visit
www.forecastinternational.com or call +1 203.426.0800

Cyber Operations

Outlook

- Cybersecurity is a growing field and is critical to protecting America's nuclear missile arsenal
- Funding is primarily provided by DARPA in classified programs, making it difficult to discern the specifics of funding allocations
- Funding fluctuates as new technology is developed and replaced as cyberattacks proliferate
- Major funding influx into the mid- to late 2020s



Orientation

Description. The U.S. Missile Defense Agency's Cyber Operations project conducts a variety of cyber research, testing, analysis, and risk assessment activities.

Status. Ongoing research, development, and testing.

Application. Cyber operations for the U.S. Missile Defense Agency.

Sponsor

U.S. Missile Defense Agency
 5700 18th St, Bldg 245
 Fort Belvoir, VA 22060-5573
 USA

Contractors

Prime

Lockheed Martin Space Systems - Sunnyvale	http://www.lockheedmartin.com , 1111 Lockheed Martin Way, Sunnyvale, CA 94088-3504 United States, Tel: + 1 (408) 742-4321, Prime (Cyber Operations Ballistic Missile Defense Terminal Defense Segment)
Torch Technologies Inc	http://www.torchtechnologies.com , 4090 Memorial Pkwy SW, Huntsville, AL 35802 United States, Tel: + 1 (256) 319-6000, Fax: + 1 (256) 319-6016, Second Prime (Cyber Operations Ballistic Missile Defense Terminal Defense Segment)

Contractors are invited to submit updated information to Editor, International Contractors, Forecast International, 75 Glen Road, Suite 302, Sandy Hook, CT 06482, USA; rich.pettibone@forecast1.com

Cyber Operations

Technical Data

The Cyber Operations project sustains MDA Risk Management Framework (RMF) and Controls Validation Testing (CVT) activities. More generally, it sustains all activities necessary to comply with the Federal Information Security Management Act (FISMA). The project also provides analysis of validation results and risk assessment, and reviews of proposed Program Manager/Information Assurance

Manager Plans of Action and Milestones for MDA THAAD mission systems. The project also supports THAAD authorizations to operate in the Missile Defense System. Current efforts involve development of robust cybersecurity for both offensive and defensive purposes to address the advanced threat.

The Cyber Operations project is part of PE#0603881C (Ballistic Missile Defense, Terminal Defense Segment).



Testing Cyber Operations Technology and Security

Source: U.S. Air Force

Program Review

The Cyber Operations project was initiated in FY14. Its initial activity involved cybersecurity and information assurance engineering and architecture planning. During FY15, the project began developing and testing cybersecurity and IA control measures for Terminal High Altitude Area Defense (THAAD) systems. These efforts are ongoing.

From FY16-FY18, the project assessed whether the THAAD enclaves are adequately implementing and maintaining IA controls. In FY19, the project began updating THAAD software and hardware to ensure compliance with DoD Weapon System Information Assurance programs.

FY20 plans focused on improving software development efforts for more robust offensive and defensive cybersecurity in order to address modern, advanced threats. For FY21, the project continued the software development efforts that began in FY20. The project saw an increase in funding in FY21 and FY22 to provide the cybersecurity required in order for software development efforts to align with Missile Defense Agency priorities.

The FY24 budget provides additional funding for System Build 5.0 cybersecurity and infrastructure updates. These seek to improve the THAAD cyber posture required to ensure continuity of Authority to Operate (ATO) approvals and compliance with DoD cybersecurity requirements.

The Cyber Operations project comprises several recurring efforts undertaken with yearly budget allotments. The first, as mentioned above, is the conduct of cybersecurity and IA engineering and architecture planning for THAAD information technology systems. As also indicated above, funding has also been allocated for the development and testing of cybersecurity and IA control measures for application on THAAD systems. Another recurring effort is the development of a THAAD risk management framework for DoD IT certification and accreditation packages. And in order to keep the project operating efficiently, funding is also allocated for annual IA reviews of the THAAD enclaves to assess compliance in implementing and maintaining IA controls.

Cyber Operations

Funding

U.S. FUNDING								
	FY23	FY23	FY24	FY24	FY25	FY25	FY26	FY26
	<u>QTY</u>	<u>AMT</u>	<u>QTY</u>	<u>AMT</u>	<u>QTY</u>	<u>AMT</u>	<u>QTY</u>	<u>AMT</u>
RDT&E (U.S. MDA)								
PE#0603881C								
Ballistic Missile Defense								
Terminal Defense Segment								
Project MC07								
Cyber Operations	-	10.353	-	12.140	-	3.189	-	3.250
	FY27	FY27	FY28	FY28	FY29	FY29	FY30	FY30
	<u>QTY</u>	<u>AMT</u>	<u>QTY</u>	<u>AMT</u>	<u>QTY</u>	<u>AMT</u>	<u>QTY</u>	<u>AMT</u>
RDT&E (U.S. MDA)								
PE#0603881C								
Ballistic Missile Defense								
Terminal Defense Segment								
Project MC07								
Cyber Operations	-	3.313	-	3.380	-	3.446		N/A

All \$ are in millions.

N/A = Not Available

Note: Additional funding likely comes from the budgets of classified programs.

Worldwide Distribution/Inventories

Cyber Operations is a project of the U.S. Missile Defense Agency.

Forecast Rationale

Only a few years ago, there were reports that U.S. missile silos were vulnerable to cyberattacks. This was due in large part to the antiquated technology used by the Department of Defense. The U.S. Missile Defense Agency took the news seriously and immediately began improving its ability to protect itself from cyberattack by investing in its Cyber Operations project.

Among its many activities, the Cyber Operations project sustains the Missile Defense Agency's Department of Defense Information Assurance Certification and Accreditation Program (DIACAP) and its Controls Validation Testing (CVT) activities. The agency also supports certification of the Terminal High Altitude Area Defense (THAAD) mission system to enable it to operate as part of the ballistic missile defense system (BMDS).

Project activity remains semi-classified. Still, funding can be expected to be steady for the next several years. Due to the increased risk of cyber threats, the project is sure to see consistent attention in the yearly budget. The recent string of cyberattacks on critical infrastructure

throughout the United States has proven this attention to be warranted. Additionally, due to the nature of the work, the COVID-19 pandemic likely had no impact on the project.

A large decrease from FY 2024 to 2025 reflects the realignment of the cyber budget for weapon system-specific cyber development, or component modification efforts from Budget Project MC07 to MD07 THAAD development accomplishment, in accordance with DoD guidance.

A wide-scale cyberattack in 2020 reaffirmed the need for improved cybersecurity. Large amounts of DoD data were compromised by hackers who were able to gain access to DoD servers by attacking the third-party developers of DoD security software. The malicious actors snuck weaknesses into regular software updates. The large-scale nature of this attack highlights the risk of the government contracting third-party developers for the creation of protected networks. It also highlights the need to increase cybersecurity efforts, as there is a possibility of such actors attacking THAAD systems.

Cyber Operations

Ten-Year Outlook

ESTIMATED CALENDAR YEAR RDT&E FUNDING (in millions US\$)												
Designation or Program		High Confidence				Good Confidence			Speculative			
	Thru 2023	2024	2025	2026	2027	2028	2029	2030	2031	2032	2033	Total
Lockheed Martin Space Systems - Sunnyvale												
Cyber Operations <> United States <> Department of Defense												
	55.41	12.14	12.78	12.14	12.55	13.44	13.50	13.75	14.00	14.25	14.50	133.05
Total	55.41	12.14	12.78	12.14	12.55	13.44	13.50	13.75	14.00	14.25	14.50	133.05