

United States Central Command Unfunded Priorities List for Fiscal Year 2024

1. Providing for Air Defense

a. Air Vigilance (AV) Operations and Sustainment:

(U) EXECUTIVE SUMMARY. Countering Unmanned Aerial Systems (UAS) is a top USCENTCOM priority. State and non-state actors continue to mature their UAS capabilities, tactics, techniques, and procedures at an alarming rate and present a direct threat to the United States and its regional partners and allies.

(U) The Air Vigilance (AV) system delivers a ground-based passive signals intelligence sensor employed to detect, track, identify, geo-locate, and report UAS threat activities. Within the USCENTCOM area of responsibility (AOR), 18 AV systems in 8 countries provide force protection capability for both forces and critical infrastructure.

b. CRESTONE UxS Database Inventory:

(U) EXECUTIVE SUMMARY. CRESTONE is being used operationally throughout the USCENTCOM AOR to identify and track specific signals of interest. Funding will be used to hire additional engineers, shorten testing timelines, and expand the signal of interest library capacity to enhance defeat options against the UAS threat throughout the USCENTCOM AOR.

(U) OPERATIONAL IMPACT / RISK TO the National Defense Strategy (NDS). Additional investment in AV and CRESTONE sustains operational capability to collect critical intelligence data on emerging aerial threat systems and provide early warning of operations in restricted airspace. The requested funding supports the required communications transport layer and the maintenance services for power, heating-ventilation-air conditioning, and Intrusion Detection Systems. Any loss or degradation of our ability to collect and report on adversarial attack vectors and share collected data with other Geographic Combatant Commanders increases operational risk to US and Partner Forces.

Priority	USCENTCOM FY23 Unfunded Priorities Budget Line Item Number (LIN)	Sub-Activity Group (SAG)	Program Element (PE) Number	Amount (\$M)
1	Tactical Electronic Surveillance System – Adv Development / Air Vigilance Operations and Sustainment	121	0603766A	\$14.7
	AF TENCAP / CRESTONE Database	012C	0207247F	\$15.0

2. Building Joint Force Resiliency / Agile Logistics

(U) Prepositioned War Reserve Materiel (PWRM) Stockpile Readiness:

(U) EXECUTIVE SUMMARY. Sufficient PWRM stocks are a necessity in compensating for the lack of forces and footprint in theater. Additional investment will help build a long-term enduring advantage in managing risk and preparing to respond to small-scale, short-duration crises without substantially impairing high-end warfighting readiness caused by the diversion of

United States Central Command Unfunded Priorities List for Fiscal Year 2024

resources. Contingency preparedness in the form of PWRM readiness is foundational to deterrence. Mobile prepositioned stocks are critical to quickly stand up temporary and smaller-scale logistical support locations near the point of use as conflict unfolds.

(U) OPERATIONAL IMPACT / RISK TO NDS. Without PWRM levels requested, USCENTCOM is unable to fully meet contingency plan operational base requirements in the specified time period. Funding is critical to filling shortages of bed-down and life support systems, fuel support distribution and storage equipment, and rapid runway repair sets. The requested \$125.1M will replenish PWRM stockpiles up to the quantity required to achieve a C-1 readiness rating.

Priority	USCENTCOM FY24 Unfunded Priorities Budget Line Item Number (LIN)	Sub-Activity Group (SAG)	Program Element (PE) Number	Cost (\$M)
2	Expeditionary Airfield Basing Assets (BEAR, AGE, RADR)	021D	0401135F	\$82.2
	WRM Equipment / Secondary Items (Fuels Support Equip)	021D	0208031F	\$25.6
	Globally Positioned Network USCENTCOM (GPN-CENT)	041Z	0708550F	\$16.0
	WRM Equipment / Secondary Items (APS-5)	212	0208031A	\$4.1

3. Innovation

a. Data Analysis and Artificial Intelligence (AI) Initiative Baseline:

(U) EXECUTIVE SUMMARY. Additional investment is critical in moving USCENTCOM towards leveraging data as a strategic asset. USCENTCOM’s military advantage is increasingly reliant on data-driven technologies and the integration of diverse data sources, elastic computing to the edge, and rapid software deployment. Data provides new ways and means to monitor, respond, and deter aggression at the speed of operations.

(U) OPERATIONAL IMPACT / RISK TO NDS. Request \$8M to recruit data scientists and provide hardware and technology capable of processing large amounts of code, and data libraries.

b. Maven Smart System (MSS) Enterprise Licenses:

(U) EXECUTIVE SUMMARY. USCENTCOM’s military advantage is increasingly reliant on data-driven technologies and the integration of diverse data sources, elastic computing to the edge, and rapid software deployment. Information sharing and data analytics are principal mechanisms for understanding China’s encroachment, illuminating Russia’s activities, disrupting Iran’s UAS / Advanced Conventional Weapons (ACW) supply chains, and spoiling ISIS and AQ external operations.

United States Central Command Unfunded Priorities List for Fiscal Year 2024

(U) OPERATIONAL IMPACT / RISK TO NDS. Funding provides USCENTCOM with an enterprise license for users of MSS. MSS allows users to explore and visualize the battlefield while increasing ability to anticipate, monitor, and respond to destabilizing activities from strategic competitors. Leveraging MSS as a strategic asset provides new ways and means to monitor, respond, and deter aggression at the speed of operations.

c. Cloud Computing Environment / Cloud Transition:

(U) EXECUTIVE SUMMARY. Cloud Computing Environment is the foundation upon which USCENTCOM builds and tailors effective cyber security, advanced analytical capabilities, command and control, and future enabling technologies. USCENTCOM cloud strategy focuses on agility, flexibility, and modernization. Rapid delivery of enterprise resources and services result in an organization equipped to respond and fight in the digital age. When mission needs change, a flexible cloud-based IT enterprise can rapidly scale or reallocate resources or react and remediate incidents. The desired end state is to establish a multi-vendor, multi-cloud ecosystem that hosts both on- and off-premise services across all classification levels.

(U) OPERATIONAL IMPACT / RISK TO NDS. Funding facilitates USCENTCOM’s migration to this new capability and provides resources to leverage existing systems, and develop tools and protocols for secure operations and applications. Without these funds, USCENTCOM falls short of meeting DoD CIO mandates. USCENTCOM and coalition partner operations are put at risk due to increased network security threats due to the inability to securely manage and implement critical software / firmware updates on all networks and systems throughout the Command.

Priority	USCENTCOM FY24 Unfunded Priorities Line Item Number (LIN)	Sub-Activity Group (SAG)	Program Element (PE) Number	Amount (\$M)
3	CCMD Direct Msn Support / Data Analysis and AI Initiative	015F	0201138F	\$8.0
	CCMD Direct Msn Support / MSS Licenses	015F	0201138F	\$34.0
	CCMD Direct Msn Support / Cloud Transition / Computing	015F	0201122F	\$30.0

4. Active Campaigning:

(U) EXECUTIVE SUMMARY. Originally fielded in 2015, Full Motion Video Extension Unified Relay (FEURY) remains a critical enabler of precision strikes, force protection, and mission command within the Combined Joint Operations Area (CJOA). Since January 2022, seven (7) Operation Inherent Resolve (OIR) FEURY sites have enabled 53 airstrikes, linked to 1,779 Rover feeds, and supported 5,672 total mission hours in the ongoing fight against Da’esh and Iranian-Aligned Militia Groups (IAMG). The situational awareness that FEURY provides is vital to the exercise of mission command, even when not resulting in an airstrike. In January 2022, FEURY provided decision makers and operators real-time, situational awareness of a prison break in Syria. FEURY was a vital link in coordinating ground force responses used to

United States Central Command Unfunded Priorities List for Fiscal Year 2024

contain the situation. FEURY also gives Combined Joint Task Force-Operation Inherent Resolve (CJTF-OIR) the ability to monitor politically sensitive sites and the Iraqi forces the ability to leverage their airpower in protecting US forces in a theater constrained by Force Manning Level (FML) limits and competing NDS priorities.

(U) OPERATIONAL IMPACT / RISK TO NDS. Service funding support for seven (7) FEURY nodes in the USCENTCOM AOR ends in November 2023. CJTF-OIR requires support for these seven FEURY nodes for an additional year to preclude gaps in Full Motion Video (FMV) capability while alternative means for providing similar capability is pursued. Complete loss of FEURY FMV would severely degrade CJTF-OIR’s ability to identify and prosecute targets, execute mission command, and place personnel and CJTF-OIR missions at risk.

Priority	USCENTCOM FY24 Unfunded Priorities Budget Line Item Number (LIN)	Sub-Activity Group (SAG)	Program Element (PE) Number	Amount (\$M)
4	Agile ISR / Full Motion Video Extension Unified Relay (FEURY)	011C	0305206F	\$12.0

5. Digital Modernization

(U) EXECUTIVE SUMMARY. USCENTCOM Digital Modernization is essential to the Command’s ability to maintain information and decision advantage, preserve C4 systems, and ensure critical kill chains. USCENTCOM’s Digital Modernization plan applies Department of Defense (DoD) Digital Modernization Strategy (June 5, 2019) principles to develop its Future Mission Environment (FME). The FME is an essential element for integrating USCENTCOM into Joint All Domain Command and Control (JADC2) and the DoD Mission Partner Environment (MPE).

(U) OPERATIONAL IMPACT / RISK TO NDS. FME replaces legacy counter-violent extremist organization-oriented capabilities developed over the past three decades that tether the Command to fixed information technology hubs that are becoming increasingly vulnerable to state-based adversaries. FME implementation requires several Digital Modernization enhancements.

a. Zero Trust Architecture (ZTA) / Internet Protocol v6:

(U) EXECUTIVE SUMMARY. In existing USCENTCOM networks, users and endpoint devices are automatically trusted within the perimeter and put the organization at risk from malicious internal actors and those with assumed legitimate credentials with unauthorized and compromised accounts-wide access within the network.

(U) OPERATIONAL IMPACT / RISK TO NDS. With ZTA funded, USCENTCOM will be able to implement networks that leverage micro-segmentation, security monitoring and response, and general protective / preventative controls that improve an organization's cyber security posture and reduce risk.

United States Central Command Unfunded Priorities List for Fiscal Year 2024

b. Software Defined Networks:

(U) EXECUTIVE SUMMARY. Software Defined Networks (SDN) use software-based controllers or application programming interfaces (APIs) to communicate with underlying hardware infrastructure to direct network traffic. Use of this approach is directed in the DoD Zero Trust Reference Architecture / Software Defined Networking (SDN), December 2020. SDN benefits include cost savings realized through reductions in time spent on manual tasks and improved utilization of existing USCENTCOM network resources.

(U) OPERATIONAL IMPACT / RISK TO NDS. Not resourcing SDN critically degrades operational availability and uptime / loading of software upgrades to all USCENTCOM networks. SDN speeds system recovery times and reduces USCENTCOM networks failure rates.

c. Army Intelligence Information Technology (IT) Systems and Networks:

(U) EXECUTIVE SUMMARY. United States Army Central Command (USARCENT funding to support Army Intelligence IT Systems and Networks has been decremented 100% in PB24. USARCENT requires \$5M for the information security systems necessary to protect DoD intellectual property and technical advances.

(U) OPERATIONAL IMPACT / RISK TO NDS. Without additional funding, the Joint Worldwide Intelligence Communication System (JWICS) network and system support would collapse. The number of organic military personnel with the appropriate Military Occupational Specialty are insufficient to fill the contract void. The loss of JWICS support to OIR and Operation Spartan Shield (OSS) would result in an unacceptable loss of actionable intelligence to support targeting, force protection, collection management, and threat monitoring across the AOR.

d. (U) Army Strategic Network Transport:

(U) EXECUTIVE SUMMARY. USARCENT requires Command, Control, Communications, Computer, Information Technology (C4IT) infrastructure in order to direct operations, access information needed for situational awareness, decision-making, and maintain the ability to exchange information in a contested environment. In this role, USARCENT provides the C4IT capabilities and infrastructure in the Southwest Asia (SWA) Theater supporting OSS and CJTF-OIR. To meet these requirements, USARCENT requires resources for SWA network modernization, sustainment, and service support necessary to meet the Theater's on-going and future operational requirements. Recent Theater transition, both operational and budgetary, has led to a gap in required funding in PB24 placing risk on USARCENT's ability to operate, maintain, modernize, and defend the SWA network.

(U) USARCENT provides SWA network support across theater via Commercial Satellite leases, Terrestrial Fiber leases, SWA Theater Signal Service Support, and Field Service Representatives (FSR). These capabilities require sufficient funding to support USARCENT, Joint, and Coalition operations across SWA. The decrements to these requirements present a

United States Central Command Unfunded Priorities List for Fiscal Year 2024

high risk to the USARCENT mission to provide C4IT capabilities in support of on-going operational requirements. Failure to fund affects the two highest priority requirements that support strategic communications – commercial satellite and terrestrial fiber leases.

(U) OPERATIONAL IMPACT / RISK TO NDS. Without an additional \$25.3M in FY24, USARCENT will be unable to lease the primary and alternate means of transporting data to the Department of Defense Information Network (DoDIN) and source FSRs to maintain the network. Lack of funding reduces USARCENT’s ability to protect and defend the SWA strategic network against cybersecurity threats on all voice, video, and data services across the Non-Secure Internet Protocol Router (NIPR), Secure Internet Protocol Router (SIPR), and coalition networks. This translates to degraded command and control and increased risk to operations in what remains a very kinetic and dynamic theater.

Priority	USCENTCOM FY24 Unfunded Priorities Line Item Number (LIN)	Sub-Activity Group (SAG)	Program Element (PE) Number	Amount (\$M)
5	USCENTCOM Communications / Zero Trust Architecture, IPv6	015F	0201122F	\$5.5
	USCENTCOM Communications / Software Defined Networks	015F	0201122F	\$3.4
	Military Intel Program (MIP) Activities / Army Intel Info Systems and Networks	411	0305192A	\$5.0
	Army IT Services Mgt C2 Systems Defense Enterprise Wideband SATCOM / Army Strategic Network Transport	121	0208550A	\$2.3
		122	0310700A	\$23.0