MARK E. GREEN, MD, TENNESSEE
CHAIRMAN

BENNIE G. THOMPSON, MISSISSIPPI
RANKING MEMBER

One Hundred Nineteenth Congress
Committee on Homeland Security
U.S. House of Representatives
Washington, DC 20515

July 1, 2025

The Honorable Admiral Kevin E. Lunday
Acting Commandant
U.S. Coast Guard
2703 Martin Luther King Jr. Avenue SE
Washington, D.C. 20593

Dear Admiral Lunday:

The United States faces an increasingly complex and contested threat environment across multiple regions, where adversaries are employing unmanned aircraft systems (UAS), loitering munitions, and autonomous drone swarms to challenge American military presence, disrupt international commerce, and undermine the rules-based international order.

In the wake of Iran's retaliatory missile attacks on U.S. installations in Qatar, following President Trump's successful and justified strike on Iranian nuclear infrastructure, it has become clear that American forces deployed in the Middle East, including U.S. Coast Guard personnel, are operating within a rapidly escalating domain of aerial and asymmetric threats.[1] As Congress continues to assess the force protection posture of our forward-deployed assets, we must ensure the Coast Guard is equipped with the tools, authorities, and capabilities necessary to defend against this new generation of threats, not only in the Middle East, but increasingly in the Indo-Pacific, where the People's Republic of China (PRC) is aggressively fielding its own advanced drone capabilities.

Recent reporting indicates that Iranian missile attacks against Al Udeid Air Base, where U.S. and coalition forces are stationed, were swiftly intercepted, followed by an unprecedented Qatari-brokered ceasefire between Israel and Iran.[2] Yet the events of last week demonstrate how quickly the regional security environment can deteriorate, and how U.S. forces, including Coast Guard cutters deployed under Patrol Forces Southwest Asia (PATFORSWA), may become targets of hostile state or proxy drone and missile operations. Iran and its partners have demonstrated the ability to deploy weaponized drones from land, sea, and air platforms with increasing sophistication, blurring the lines between conventional and irregular warfare.[3]

---

[1] Matthew Cullen, "*Iran Sends Heat Wave of Missiles at U.S. Base in Qatar, Then Halts*," The New York Times, June 23, 2025, https://www.nytimes.com/2025/06/23/briefing/iran-us-base-heat-wave.html.
[2] Adam Rasgon, "*Iran and Israel Agree to Cease-Fire in Qatar-Mediated Deal*," The New York Times, June 23, 2025, https://www.nytimes.com/2025/06/23/world/middleeast/iran-israel-ceasefire-qatar.html.
[3] Jon Gambrell, "*Yemen's Houthi Rebels Launch Drone Boat That Hits Ship in Red Sea*," Associated Press, August 23, 2024, https://apnews.com/article/yemen-houthi-rebels-red-sea-attacks-israel-hamas-war-2faa48176d4f773003b6a4a3ad5ca73d.

Information obtained through recent House Committee on Homeland Security oversight efforts involving the Coast Guard's activities in the U.S. Central Command (CENTCOM) area of responsibility (AOR) suggests that the Coast Guard may have access to systems such as the Ninja Gen2 Counter-UAS platform and the Drone Restricted Access Using Known Electromagnetic Warfare (DRAKE) system aboard vessels in the CENTCOM AOR.[4] However, it is unclear whether these systems offer a complete kill-chain capability, spanning detection, identification, tracking, disruption, and kinetic defeat, or if they are limited to surveillance or electronic disruption alone. Even where electronic warfare (EW) tools are employed, concerns persist regarding their range, reliability, and performance in high-interference or contested electromagnetic environments. Equally unclear is whether these systems are organically owned and operated by the Coast Guard or temporarily assigned from the U.S. Navy or other joint entities. If the latter, this raises important questions about sustainment, accessibility, interoperability, and operational independence during a rapidly unfolding threat scenario.

These concerns are not confined to the Middle East. In the Indo-Pacific, the PRC has invested heavily in a vast network of surveillance and strike-capable drones, including those deployed aboard coast guard, maritime militia, and naval vessels. Chinese drones have been used to harass and intimidate foreign navies, intrude into the airspace of Taiwan and neighboring countries, and conduct persistent surveillance in the South and East China Seas.[5] As tensions rise across the First Island Chain, Coast Guard forces operating in the region, whether aboard National Security Cutters, Fast Response Cutters, or in support of joint maritime operations, must be prepared to encounter unmanned threats similar to those now facing their counterparts in the Persian Gulf.

Due to the complex threat environment, and to inform the Committee's oversight of Coast Guard readiness, technology adoption, and interagency coordination, we respectfully request a written response to the following questions no later than July 15, 2025:

1. What specific counter-UAS (C-UAS) systems are currently installed or accessible aboard Coast Guard cutters and facilities operating under PATFORSWA? Please detail whether these systems are Coast Guard-owned, Navy-loaned, or Joint Force allocated, and describe their full range of operational capabilities (i.e., detection, identification, jamming, or kinetic defeat).

2. Do any of the C-UAS platforms deployed by the Coast Guard in the Middle East possess autonomous or integrated kill-chain capability? Specifically, are they able to detect and neutralize drone threats without cueing from external platforms? What is the effective range of these systems, and are they capable of engaging high-speed, low-altitude, or swarm-based threats?

---

[4] U.S. Coast Guard personnel, briefing to congressional staff, Manama, Bahrain, October 8, 2024.
[5] Dzirhan Mahadzir, "*Chinese Drones, Surveillance Aircraft Step Up Patrols Near Taiwan, Philippine Sea*," USNI News, April 29, 2025, https://news.usni.org/2025/04/29/chinese-drones-surveillance-aircraft-step-up-patrols-near-taiwan-philippine-sea.

3. What organic EW capabilities does the Coast Guard possess to disrupt or neutralize hostile UAS in real time, including but not limited to directed-energy systems, radio frequency jamming, spoofing, or signal manipulation tools? Are these EW capabilities deployed aboard Coast Guard vessels independently, or do they rely on integration with U.S. Navy or joint force systems? Please assess their operational reliability and effectiveness in denied or contested electromagnetic environments.

4. Has the Coast Guard conducted a formal capability gap analysis or red-team evaluation of its vulnerability to drone and loitering munition attacks in the CENTCOM area of operations? If so, what deficiencies were identified, and what mitigation steps have been taken?

5. What contingency protocols are in place in the event of a successful drone or missile strike on a Coast Guard cutter or forward-deployed infrastructure in Bahrain or surrounding waters? Do these protocols account for degraded communications, mass casualty response, or simultaneous multi-vector attacks?

6. What C-UAS training, rules of engagement, and operational authorities are currently issued to Coast Guard personnel operating in high-threat regions such as the Middle East and Indo-Pacific? Is this training standardized across deployed crews, and does it incorporate simulation or live-fire exercises under joint command structures?

7. What level of operational integration currently exists between the Coast Guard, the U.S. Navy's Fifth Fleet, and CENTCOM for real-time UAS threat detection, tracking, data fusion, and response coordination? Are Coast Guard systems and personnel fully integrated into theater-wide C2 networks, such as the Joint All-Domain Command and Control (JADC2) architecture?

8. Are any C-UAS systems currently deployed or planned for deployment aboard Coast Guard assets in the Indo-Pacific region, particularly those operating in contested zones near the PRC's maritime boundaries or areas of increased drone activity? If not, what resources or support would be required to address that gap?

As the Coast Guard's strategic footprint continues to grow in forward-deployed areas, so too must its ability to defend its platforms, personnel, and missions from technologically advanced adversaries. Whether operating alongside the U.S. Navy in the Persian Gulf or supporting allies in the Indo-Pacific, the Coast Guard's evolving role demands C-UAS and EW capabilities that match the threat environment it now confronts.

It is essential that Congress receive a full accounting of current gaps and resourcing needs so that we may take appropriate steps to protect our service members and preserve our maritime operational advantage. To that end, we also request that the Coast Guard provide a classified briefing to the Committee by no later than July 18, 2025.

An attachment contains instructions for responding to this request. To the maximum extent possible, please provide unclassified responses to these requests. Any classified information provided in response to this letter should be provided under separate cover.

Please contact Homeland Security Committee Majority staff at (202) 226-8417 with any questions about this request.

Thank you for your attention to this important matter and your prompt reply.

Sincerely,

MARK E. GREEN, M.D.
Chairman
Committee on Homeland Security

CARLOS A. GIMENEZ
Chairman
Subcommittee on Transportation
and Maritime Security

SHERI BIGGS
Member of Congress

Encl.

cc: The Honorable Bennie Thompson, Ranking Member
Committee on Homeland Security

The Honorable LaMonica McIver, Ranking Member
Subcommittee on Transportation and Maritime Security