U. S. Department of Homeland Security

United States Coast Guard

Commandant
United States Coast Guard

2703 Martin Luther King Jr Ave SE
Washington, DC 20593-7000
Staff Symbol: CG-092
Phone: (202) 372-4411
FAX: (202) 372-8302

TESTIMONY OF

REAR ADMIRAL DAVID C. BARATA
DEPUTY COMMANDANT FOR OPERATIONS POLICY
AND
REAR ADMIRAL JASON P. TAMA
COMMANDER, COAST GUARD CYBER COMMAND

ON
"CHANGES IN MARITIME TECHNOLOGY: CAN THE COAST GUARD KEEP UP?"

BEFORE THE
HOUSE TRANSPORTATION AND INFRASTRUCTURE
SUBCOMMITTEE ON COAST GUARD AND MARITIME TRANSPORTATION

December 16, 2025

Introduction

Good afternoon, Chairman Ezell, Ranking Member Carbajal, and distinguished members of the Subcommittee. Thank you for your strong support of the U.S. Coast Guard. We are honored to appear before you today to update you on Coast Guard activities related to advances in maritime technology.

The Coast Guard remains committed to ensuring our Nation's safety, security, and prosperity. The Secretary of the Department of Homeland Security (DHS) and the Acting Commandant of the Coast Guard have set us on a clear course to ensure the U.S. Coast Guard remains the world's premier Coast Guard, focused on controlling, securing, and defending the U.S. borders and maritime approaches; facilitating the flow of commerce vital to economic prosperity; and responding to crises and contingencies. We see that acquiring, integrating, and utilizing emerging maritime technologies is a critical enabler to these outcomes. Through Force Design 2028 and historic investments in the One Big Beautiful Bill Act, the Coast Guard is accelerating and increasing the adoption and deployment of new technologies to counter evolving threats and enhance mission execution. Thanks to these two initiatives, as well as continued support from Congress, we are now better postured to meet the increasing demands, threats, and promises, of emerging technology.

Emerging technology – such as autonomous systems and the use of alternative fuels — have the potential to unlock efficiencies that will reshape the Marine Transportation System (MTS), improve the flow of commerce, and increase our national security. However, with these advancements come the potential for significant cybersecurity risks which must be mitigated to protect the safety of the American people. As these technologies bring both significant economic opportunities and risk of critical vulnerabilities, the Coast Guard is diligently balancing the need to encourage innovation with its duty to prevent nefarious use of these technologies through appropriate levels of oversight and regulation.

The Coast Guard will continue to closely evaluate emerging and experimental technologies and support their safe evolution and eventual incorporation into the Coast Guard, and the MTS, through continuing dialogue across the interagency, maritime industry, and Congress.

Coast Guard Autonomous and Experimental Maritime Technology

As part of Force Design 2028, on July 1, 2025, the Coast Guard established the Robotics and Autonomous Systems (RAS) Program Executive Office (PEO). The RAS PEO consolidated multiple offices into one cohesive program dedicated to the acquisition and integration of autonomous capabilities across all Coast Guard missions and domains. The RAS PEO will expedite the implementation and operationalization of the Coast Guard's Unmanned Systems Strategic Plan.

The Coast Guard currently maintains three unmanned aircraft system (UAS) lines of effort: Long-Range UAS, Medium-Range UAS, and Short-Range UAS. As part of a joint partnership with U.S. Customs and Border Protection (CBP), the Coast Guard operates CBP's fleet of Long-Range UAS from a Joint Program Office located at CBP's National Air Security Operations Center San Angelo, TX. The Medium-Range UAS program currently uses contractor-owned, contractor-operated UAS to provide maritime UAS capability on board Coast Guard National Security Cutters. To date, the Medium-Range UAS supported the interdiction of more than $6 billion of illegal drugs, assisted in enforcement of commercial fishing laws, and supported search and rescue operations. The Short-Range UAS effort uses small quadcopter or fixed wing UAS as force multipliers in myriad operations, including post-storm assessments, law enforcement, pollution response, port and facility inspections, aids to navigation inspections, and near-shore maritime domain awareness. The Coast Guard currently operates more than 300 drones, flown by over 600 trained operators at nearly 100 separate units.

The Coast Guard's domestic counter UAS capabilities protect covered facilities and assets from potential UAS threats. The capabilities are currently limited to two deployable suites and one cutter-based system. The two suites are operated by Coast Guard Maritime Security Response Teams East and West. In September 2025, the Service allocated $150 million in funding provided by the One Big Beautiful Bill Act to bolster its counter UAS capability and align with our vision for tactical maritime domain awareness under the Service's Coastal Sentinel initiative.

Additionally, the Coast Guard employs contractor-owned and operated surface autonomous vessels to increase maritime domain awareness. The Service most recently awarded a fixed price contract for a three-year period of performance to continue this capability. Contracted deployments offer the opportunity to enhance maritime domain awareness while avoiding prolonged acquisition processes and preserving the ability to quickly pivot to emerging technologies. Furthermore, the Coast Guard Research and Development Center (RDC) and Blue Technology Center of Expertise advise the Service on technological feasibility and implementation strategies of surface autonomous vessels. The RDC is coordinating with interagency and industry partners, including the Defense Innovation Unit and the U.S. Navy's Surface Warfare Centers, to explore the expanded deployment of autonomous surface capabilities. This includes collaborative efforts to drive advances in autonomous vessel behaviors, Coast Guard-specific mission execution, and intelligent data transport.

Looking to the future, the One Big Beautiful Bill Act provides historic funding for the Coast Guard including $266 million for procurement and acquisition of organic Long-Range UAS and $75 million to contract the services of, acquire, or procure autonomous maritime systems. The Coast Guard is evaluating all Long-Range UAS solutions and options to best meet Coast Guard missions. In addition to the acquisition of multiple Long-Range UAS and support infrastructure, the Coast Guard is evaluating current maritime domain dominance and operational needs to determine what state of the art technologies are suitable for closing the Service's capability gaps. We appreciate the continued Congressional support to effectively implement autonomous maritime technologies across all Coast Guard missions to control, secure, and defend the United States border and maritime approaches, facilitate commerce vital to economic prosperity, and sustain readiness for crisis response.

Commercial Autonomous and Remote Maritime Technology

The Coast Guard is working with industry and government partners to oversee the safe deployment and use of autonomous and remote-controlled maritime technology. As new commercial autonomous vessels increase in size, complexity, and quantity, and more frequently share the waterways with one another, conventional vessels, and other waterway users, the technology will likely increase safety risk to the MTS. There are also cybersecurity risks associated with autonomous or remote-controlled vessels related to their need for advanced computing and communication technology.

Nearly all of the Coast Guard's statutory authorities and regulations for commercial maritime operations were enacted or issued on the premise of seafarers being physically on-board vessels. They do not contemplate uncrewed operations. Nevertheless, the Coast Guard is working within these existing authorities, some of which are decades-old, to safely integrate autonomous and remote-controlled technologies into the maritime domain. While simultaneously developing new domestic and international frameworks, there is a need to mitigate risk within the current legal regime.

Internationally, the Coast Guard is leading U.S. efforts within the International Maritime Organization (IMO) to develop a set of *voluntary* guidelines for the safe and secure operation of autonomous or remote-controlled cargo ships. The Maritime Autonomous Surface Ship (MASS) Code will apply to commercial cargo vessels on international voyages and supplements the existing international requirements for their design and operations. The MASS Code is expected to be finalized and adopted in December 2026.

Domestically, the Coast Guard is collaborating with industry to manage the increasing use of autonomous platforms and deepen our understanding of emerging technologies and operational practices on a case-specific basis. For example, the At-Sea Recovery Operations Pilot Program, authorized in the James M. Inhofe National Defense Authorization Act for Fiscal Year 2023, is helping the Coast Guard contribute to commercial maritime and space innovation. Under the pilot program's unique authorities to waive or modify Coast Guard regulations, the Coast Guard managed remote-controlled vessels deployed for rocket recovery missions. From 2023 to 2024, commercial space recovery activities surged by 33% and increased an additional 36% in 2025. In under two years, the Coast Guard documented over 115 missions, gathering vital data on navigation safety, machinery system reliability, manning, watchkeeping, and remote operations.

By 2026, we anticipate even more advanced operations with new partnerships and technologies on the horizon. The pilot program, although not yet concluded, demonstrates that enhanced legal flexibility allows the Coast Guard to appropriately manage risk and foster technological innovation. By leveraging insights gained through these engagements, the Coast Guard is enhancing its ability to support and effectively evaluate the safety and feasibility of autonomous vessel operations.

Building on these lessons, we recognize that our efforts are part of a broader maritime transformation. Autonomous and remote-controlled vessels are a reality, and we have seen a significant uptick in the use of this technology in smaller vessels or devices for surface and subsurface data collection. These crafts, while cost-effective for their operators, also introduce security risks. Typically, smaller and lower-profile than conventional vessels, they can evade detection, challenge maritime domain awareness, and potentially impact national security. The Coast Guard is reviewing the scope of its current statutory authorities and collaborating with state and other federal authorities to identify the most efficient mechanisms to track vessels and their ownership, and therefore strengthen our maritime domain awareness. To support these efforts, the Coast Guard will create a Robotics Mission Specialist rating to serve as our experts in the operation, maintenance, and integration of robotics and autonomous systems across the Service.

As we begin working through more advanced proposals from industry, we appreciate the opportunity for further engagement and continued Congressional support in aligning the Coast Guard's authorities with this dynamic technology.

Cybersecurity

The Coast Guard Cyber Command (CGCYBER) is charged with defending Coast Guard networks, protecting the MTS, and enabling operations in cyberspace. To help protect the MTS, CGCYBER conducts cybersecurity assessments, threat hunts, and incident response across our ports, waterways, and maritime adjacent infrastructure. CGCYBER employs a layered, collaborative, and systems-based approach, working closely with Coast Guard Captains of the Port plus federal, state, and industry partners to assess threats and vulnerabilities, determine risks, and develop mitigation strategies.

The Coast Guard's unique mix of authorities, capabilities, and partnerships allows for a comprehensive approach to cybersecurity. As co-Sector Risk Management Agency for the MTS, overall Coast Guard efforts include addressing cybersecurity through our broad regulatory, law enforcement, and assistance authorities, and its role as a part of the Joint Force. The Coast Guard's approach helps sealift capabilities that enable U.S. Armed Forces to project power, and it facilitates vital national commerce at our Nation's busiest ports.

The increasing interconnectedness of maritime systems, particularly with the integration of emerging technologies like vessel connectivity, cloud computing, autonomous systems, and the use of artificial intelligence in areas like port logistics and data analysis, presents new attack vectors. The Coast Guard is at the forefront of this battleground, proactively working to identify vulnerabilities and weaknesses in critical infrastructure and key resources (CIKR) before exploitation can cause a major incident. We are working with industry to implement robust cybersecurity standards and best practices, ensuring the secure integration of these advanced technologies into the MTS.

Our 2024 annual Cyber Trends & Insights in the Marine Environment report reveal persistent challenges that demand continuous attention. Cybersecurity hygiene issues, such as easily compromised passwords readily available to adversaries, services exposed to the internet containing exploitable vulnerabilities, and outdated, unpatched systems in both Information Technology (IT) and Operational Technology (OT) systems, continue to be prevalent. Observed cybersecurity gaps and risks in commercial IT and OT may also exist in autonomous systems as industry moves to innovate and streamline operations.

The Coast Guard is committed to proactive engagement to ensure that innovation is integrated securely and responsibly into the maritime domain. Our mission partners in this effort are diverse and include MTSA-regulated facilities and vessels, private and public maritime industry partners, port facilities, terminal operators, bulk/liquid/barge facilities, and even energy and water/wastewater treatment facilities with a maritime nexus. This includes actively engaging with emerging technologies that are rapidly transforming the MTS. This collaboration extends to international operations, where we work with partner nations to share threat intelligence, develop common cybersecurity standards, and conduct joint exercises to improve our collective ability to respond to cyber incidents in the maritime domain.

The Coast Guard is also working to strengthen its regulatory authorities to address cyber risks. On February 26, 2024, an Executive Order updated the Coast Guard's unique regulatory authorities under Title 33 of the Code of Federal Regulations, Part 6, which allow it to inspect, seize or take other security-related actions to protect U.S. vessels and waterfront facilities to expressly address cyber threats. On July 16, 2025, the Coast Guard's new cybersecurity rule for facilities and U.S. vessels went into effect. This regulation requires facilities and vessels to create cybersecurity plans and establishes a baseline cybersecurity framework to help the maritime industry prevent, detect, and respond to cyber threats.

To enhance our cybersecurity posture, the Coast Guard coordinates and operates with other members of the Joint Force at all times, leveraging our collective defensive and offensive expertise and capabilities to address sophisticated cyber threats. This includes employing the Coast Guard's newly commissioned Offensive Cyber Operations team, the 1915 National Mission Team, currently aligned under the Cyber National Mission Force at U.S. Cyber Command. In addition, Coast Guard Cyber Protection Teams are currently deployed in ports throughout the country providing highly specialized cybersecurity risk assessments and threat hunting engagements of facilities and vessels, directly supporting improvements in our critical maritime infrastructure cybersecurity posture. The Coast Guard also works closely with key Department of Homeland Security partners including the Cybersecurity and Infrastructure Security Agency and Transportation Security Administration, and other Sector Risk Management Agencies to ensure the cybersecurity of critical infrastructure.

We recognize that adversaries will continue to adapt to target new technologies, including autonomous systems, which will challenge both industry and regulations; therefore, CGCYBER is working to fill that gap with adaptability as a cornerstone of its approach.

Alternative Fuels

The Coast Guard is collaborating with the private sector and across the U.S. government to ensure new fuel technology is safely introduced into the MTS. While the use of liquefied natural gas is the most well-known alternative to traditional marine fuels, the maritime industry continues to explore other alternative energy sources. In the absence of regulations specific to some new fuel types, the Coast Guard leverages its existing regulations to evaluate and approve proposals for the use of alternative fuels.

The economic imperatives of the maritime industry will drive its search for cost-effective future fuel solutions. The Coast Guard will continue to engage with the industry to establish novel fuel system approvals, taking into consideration appropriate safeguards that ensure the safety and security of the MTS. The Coast Guard is also actively working with industry and interagency partners to ensure the safe development of the infrastructure required to develop, deliver, and use these new fuels. To this end, the Coast Guard recently updated guidelines on the bunkering of alternative fuels for a more risk-based approach coupled with potential for a wider spectrum of fuels. This promotes safe deployment of new technologies, greater flexibility for the commercial industry, and more efficient use of Coast Guard resources.

The Coast Guard remains heavily engaged in ongoing international efforts at the IMO to develop suitable requirements and the recently established guidance for alternative fuel options. While these alternative fuels share many similarities, each has its own unique risks and challenges that must be addressed to ensure safe use as a maritime fuel.

Domestically, the Coast Guard is partnering with the Department of Energy, the Nuclear Regulatory Commission, and the Department of State to ensure the safe and secure development of domestic maritime nuclear power, including floating nuclear power plants. The Coast Guard also contributes to the safe integration of nuclear technology in the maritime domain. Recently, the Coast Guard established a Maritime Nuclear Policy division within Coast Guard Headquarters to strengthen engagement with relevant partners and continue efforts to build a framework for domestic and international maritime nuclear policy. In addition, in 2025 the Coast Guard submitted a paper to the IMO's Maritime Safety Committee to expand and update outdated nuclear maritime propulsion regulations. These efforts support U.S. nuclear technologies and their adopters to ensure they have access to this emerging global market.

Other Novel Technology

In addition to autonomous maritime technology, several other technologies or novel applications are being developed or reimagined for commercial maritime use which may challenge the Coast Guard's existing governance models and effectiveness of safety oversight.

Wing-In-Ground effect (WIG) craft present potential opportunities for both the commercial and public sectors. These multimodal craft operate by flying just above the water, crossing between the maritime and air domains. Successfully addressing the challenges associated with this technology will require the Coast Guard to rely on the Federal Aviation Administration (FAA) and technical experts with the requisite experience, competency, and statutory and regulatory authorities to evaluate the aviation aspects associated with some new WIG craft. To accomplish this, and in accordance with the FAA Reauthorization Act of 2024, the Coast Guard is working with the FAA to develop a Memorandum of Understanding to jointly coordinate the Agencies' efforts towards the oversight of WIG craft.

The Coast Guard investigation into the loss of the *Titan* submersible, which imploded during a June 2023 dive to the RMS *Titanic* killing five people, outlines key findings and contributing factors in the casualty, and includes 17 safety recommendations aimed at strengthening oversight of submersible operations, improving coordination among federal agencies and closing gaps in international maritime standards. Several of the key findings highlight inadequate engineering design and analysis related to the novel use of a carbon fiber submersible hull, highlighting the ever-present need for Coast Guard oversight of novel commercial applications of maritime technology from design through operation.

Conclusion

The scope and speed of these new technologies, some inconceivable just a decade ago, are revolutionizing maritime commerce and the Coast Guard appreciates the criticality of the moment. As we gain experience with these novel technologies, we constantly review our authorities and work to adjust our approach to oversight where appropriate. Through investments in the Coast Guard provided in the One Big Beautiful Bill Act, and Coast Guard's Force Design 2028, we are better postured to control, secure, and defense the U.S. border and maritime approaches, facilitate commerce vital to economic prosperity, and respond to crisis and contingencies that may come with little or no warning. We look forward to answering your questions.