Chair, Vice Chair, and Members of the Committee:

Thank you for the opportunity to submit written testimony in strong support of SB825/HB1239, which establishes a Critical Infrastructure Protection Branch within the Maryland Coordination and Analysis Center (MCAC).

I previously served as the Principal Cyber Advisor for the Department of the Navy. In that role, I advised senior civilian and uniformed leadership on cyber risk, operational readiness, and the security of the systems that enable naval and Marine Corps missions worldwide. One of my leading efforts during that time was elevating awareness of a structural vulnerability that often receives insufficient attention: much of the infrastructure that enables Department of Defense mission execution is not owned or operated by the federal government. It is owned and operated by state and local governments and private industry.

Installations depend on local power grids. Shipyards depend on municipal water systems. Communications infrastructure that supports operational command and control frequently traverses commercial networks. Transportation hubs that move personnel and materiel are state-managed assets. In short, the ability of the Department of the Navy—and the broader Department of Defense—to project power depends in significant part on infrastructure that sits outside federal control. From that vantage point, it became clear to me that critical infrastructure protection is not just a federal issue. It is a state responsibility with direct national security implications. SB825/HB1239 reflects precisely that understanding.

Threats to critical infrastructure are no longer speculative. They are persistent, sophisticated, and increasingly integrated across cyber and physical domains. In recent years, activity targeting U.S. infrastructure has not only increased, but public acknowledgment of that activity by senior national security leaders has increased as well. In a recent interview on 60 Minutes, the former Commander of United States Cyber Command and Director of National Security Agency publicly discussed adversary “pre-positioning” inside U.S. critical infrastructure. He acknowledged that the People’s Republic of China has established access within portions of U.S. infrastructure—not to cause immediate disruption, but to hold those systems at risk during a potential crisis or conflict.

That is what “pre-positioning” means: gaining and maintaining access in advance, creating the ability to impose consequences at a time of their choosing. When leaders at that level speak openly about adversary presence inside infrastructure, it signals something important. This is no longer an abstract warning from analysts. It is an operational reality being addressed at the highest levels of government.

We have seen Chinese cyber actors probe energy and water systems. We have seen ransomware operations disrupt hospitals and municipal services. We have seen information operations target public confidence in essential services. These activities are not random. They are deliberate shaping operations designed to create leverage, impose costs, and constrain decision-making during a crisis. Maryland hosts military installations, federal facilities, transportation hubs, biotechnology assets, and defense contractors that would be strategically relevant in any national emergency. Pre-positioning inside infrastructure in this state would have consequences well

beyond Maryland's borders. The resilience of Maryland's infrastructure is therefore not only a matter of state governance—it is directly tied to national defense readiness. The lesson is clear: we do not get a warning shot.

Critical infrastructure is not a collection of isolated assets. It is a networked system of systems. Power supports water. Water supports hospitals. Communications support emergency services. Transportation supports supply chains. An attack on one node can cascade across sectors in ways that are difficult to predict in the moment. That reality demands organized, deliberate analysis in advance of crisis. SB825/HB1239 recognizes this by directing the state to analyze threats holistically, prioritize assets based on cascading impact, map interdependencies, develop coordinated response plans, and engage directly with critical infrastructure sector leaders. This is not duplication of existing efforts. It is integration of them.

Maryland is uniquely positioned. We host major federal facilities, defense contractors, biotechnology firms, transportation hubs, and energy infrastructure. The state's economic and national security footprint is significant. The Maryland Coordination and Analysis Center already plays a critical role in information sharing. Establishing a dedicated Critical Infrastructure Protection Branch within MCAC centralizes analytic capability focused specifically on infrastructure risk, strengthens public-private coordination before a crisis occurs, and enables prioritization based on impact rather than anecdote. In the cyber domain, speed and integration win. Organizational clarity is a prerequisite to both.

Adversaries move continuously. Bureaucracies move episodically. The question before this committee is not whether Maryland faces infrastructure risk. It does. The question is whether the state organizes proactively or waits for a catalyzing event to force reorganization under pressure. History consistently shows that it is far more expensive—financially, socially, and operationally—to rebuild resilience after a disruption than to establish coordination before one.

From my experience at the Department of the Navy, I can say with confidence that state-level infrastructure resilience is inseparable from national defense readiness. Maryland does not need to reinvent the wheel. It needs to align the spokes. SB825/HB1239 provides a mechanism to integrate analysis, prioritize risk, coordinate with industry, and prepare for cascading impacts in a disciplined and sustainable way.

The threats to critical infrastructure are real, present, and accelerating. The cost of inaction will not be measured only in dollars, but in public confidence, economic stability, and operational continuity. The question is not whether we can afford to prepare — it is whether we can afford not to. Adversaries are already organized. Maryland should be too.

Respectfully submitted,
Chris Cleary