Anne R. Kaiser
Legislative District 14
Montgomery County

Vice Chair
Appropriations Comittee

Rules and Executive
Nominations Committee

The Maryland House of Delegates
6 Bladen Street, Room 121
Annapolis, Maryland 21401
410-841-3036
800-492-7122 *Ext.* 3036
Anne.Kaiser@house.maryland.gov

THE MARYLAND HOUSE OF DELEGATES
ANNAPOLIS, MARYLAND 21401

Chair Wells and distinguished members of the Government, Labor, and Elections Committee, it is with glee that I come before you and offer testimony in favor of **House Bill 1239: Public Safety - Critical Infrastructure Protection.** This bill is a crucial step in building our defenses to protect Maryland's critical infrastructure from cyber-attacks.

Critical infrastructure refers to the economic sectors whose degradation would threaten US national security and public safety. Many of these systems are powered and controlled by *operational technology* (OT) -- the hardware and software that manage industrial processes such as power generation, water treatment, and transportation networks.

Operational technology represents one of the most significant cybersecurity vulnerabilities in critical infrastructure. Unlike traditional *Information Technology* (IT) systems, many OT systems were designed decades ago without modern safety protocols. This vulnerability is exacerbated by an institutional lack of OT expertise within agencies. A successful cyber-attack on OT systems could disrupt electricity, contaminate water supplies, halt transportation, or impair emergency services.

This risk is not hypothetical. Domestic and international actors have become increasingly skilled and aggressive in targeting American infrastructure. Recent campaigns attributed to groups such as Salt Typhoon and Volt Typhoon have demonstrated a clear intent to disrupt U.S. critical infrastructure systems. These efforts reflect a strategic shift toward holding civilian infrastructure at risk during times of conflict. *Maryland is uniquely exposed to these threats.* As home to Fort Meade, the National Security Agency, U.S. Cyber Command, and a dense concentration of federal agencies and defense contractors, Maryland represents both a strategic asset and a high-value target. At the same time, as a major cybersecurity hub for the private sector and home to some of the nation's most advanced cybersecurity programs, Maryland is in an advantageous position to respond to pressing critical infrastructure threats.

HB1239: (1) establishes the Critical Infrastructure Protection Branch in the Maryland Coordination and Analysis Center. (2) requires the Branch to coordinate with the Department of Information Technology, the Office of Security Management, the Public Service Commission, industry and military leaders, and other relevant stakeholders to identify threats to the State's critical infrastructure and strengthen the State's priority assets (3) directs the Department of Emergency Management to coordinate consequence management efforts and respond to attacks on the State's critical infrastructure (4) directs the Department of Information Technology (DoIT) allow owners of critical infrastructure to become members of the Maryland Information Sharing and Analysis Center. I am also preparing amendments to clarify DoIT and the State Chief Information Security Officer's role, as well as to reduce the fiscal note.

With this bill, Maryland will be better equipped to prevent and respond to attacks in our most critical sectors.

I urge a favorable report on **House Bill 1239**. Thank you.