Vaughn Stewart
Legislative District 19
Montgomery County

Chief Deputy Majority Whip

Government, Labor, and Elections Committee

Vice Chair
Democratic Caucus

The Maryland House of Delegates
6 Bladen Street, Room 151
Annapolis, Maryland 21401
410-841-3528
800-492-7122 *Ext.* 3528
Vaughn.Stewart@house.maryland.gov

THE MARYLAND HOUSE OF DELEGATES
Annapolis, Maryland 21401

Testimony in Support of HB 718
Information Technology - State and Higher Education E-Mail - Requirements
Testimony by Delegate Vaughn Stewart
March 10th, 2026 | Appropriations Committee

I. Introduction

I want to start with a number: **$40 million**. That is a conservative estimate of what Maryland taxpayers lose every year to a problem so familiar it no longer registers as a problem at all — spam flooding the inboxes of state and university employees. Lost minutes become lost hours. Lost hours become lost workdays. Lost workdays become a quiet, invisible drain on state resources that this legislature has the power to address.

House Bill 718 addresses it. The bill is targeted, legally sound, and fiscally responsible. I urge the Committee to issue a favorable report.

II. What the Bill Does

HB 718 accomplishes three things in plain statutory language.

First, it declares that Maryland's state and higher education employee email systems exist for one purpose: state business. "State business" is defined as activities in furtherance of a governmental unit's legal obligations and functions — not commercial solicitations, mass marketing campaigns, phishing attempts, or bulk messages bearing no relationship to the work of government.

Second, it directs DOIT and higher education institutions to adopt and enforce acceptable use policies consistent with that purpose. This is not a mandate to build new infrastructure; it is a mandate to write down — clearly, in policy — what everyone already knows to be true: work email is for work.

Third, and most consequentially from a legal standpoint, it establishes as a matter of state policy that these email systems are not public forums. That designation is not bureaucratic jargon. It is the legal mechanism that gives government the authority to restrict unsolicited

access to its communications infrastructure — and, as I will explain, it is a designation that Maryland's existing policies conspicuously lack.

III. The Fiscal Case: What Spam Actually Costs Maryland

Spam has a reputation as a minor annoyance. The data tell a different story.

Global email security researchers estimate that roughly 45% of all email sent worldwide is spam. Studies of workplace productivity — including research published by the McKinsey Global Institute and corroborated by time-motion analyses in government settings — consistently find that employees spend between 20 and 40 minutes per week managing unsolicited email: deleting it, scanning it, occasionally misidentifying a legitimate message as junk and recovering it, and in some cases clicking through it to verify a sender's identity before deleting.

Maryland's executive branch employs approximately 80,000 full-time workers. The University System of Maryland adds tens of thousands more. If we apply the most conservative end of the research — just 20 minutes per employee per week — across even half of those employees, Maryland loses more than 800,000 hours of compensated work time annually to inbox noise. At the median hourly rate of a Maryland state employee, that figure represents losses in the range of $30 to $40 million per year. Every dollar of that is a dollar of public money spent not serving Marylanders.

That is the productivity cost alone. It does not capture the cost of the security incidents spam enables.

IV. The Cybersecurity Case: Spam Is Not Just Annoying — It Is Dangerous

Phishing emails are a subset of spam, and they are the single most common entry point for cyberattacks on government systems. According to the Cybersecurity and Infrastructure Security Agency (CISA), more than 90% of successful cyberattacks begin with a phishing email. The 2021 Colonial Pipeline ransomware attack — which caused fuel shortages across the Eastern Seaboard and cost the company $4.4 million in ransom — was initiated through a single compromised credential obtained via phishing.

Maryland is not immune. State and local government agencies are among the most targeted sectors for ransomware attacks, precisely because they hold sensitive data, operate critical infrastructure, and have historically underinvested in cybersecurity compared to the private sector. When a Maryland agency employee receives and clicks a malicious link embedded in a bulk email, the exposure is not merely to that employee's account — it is a potential entry point into systems serving millions of Marylanders.

HB 718 attacks this problem at the source. By establishing a legal basis to restrict unsolicited inbound email, Maryland can more aggressively filter, block, and reject messages that have no legitimate business purpose — shrinking the attack surface available to bad actors. Every phishing email blocked before it reaches an inbox is a potential breach that never happens.

There is also a subtler risk that deserves mention. Heavy spam volume trains employees to treat their inboxes as noise — to skim and delete rather than read carefully. That habit is exactly what phishers rely on to slip fraudulent messages past human review. A cleaner inbox is not merely more productive; it is more secure, because employees who are not inundated with junk email are better positioned to notice when something unusual arrives.

V. Why Existing Policies Are Not Enough

The Department of Information Technology operates a spam filter. That is good. But a spam filter is a technical tool, not a legal framework — and the two are not interchangeable.

Consider the gap. DOIT's Acceptable Use policy — updated as recently as February 18, 2026 — prohibits uses of state IT systems inconsistent with "state business." But it does not define that term. A policy that prohibits conduct without defining the conduct it prohibits is a policy without teeth. Employees, agency heads, and — importantly — courts cannot be expected to apply a standard that the policy itself declines to articulate. HB 718 provides that definition, and it does so in statute, where it carries the force of law.

More critically, neither DOIT's spam filtering policy nor its Acceptable Use policy addresses the public forum question. This is not a minor omission. Under the First Amendment's public forum doctrine — developed by the Supreme Court in *Perry Education Ass'n v. Perry Local Educators' Ass'n*, 460 U.S. 37 (1983), and applied to government digital infrastructure in subsequent cases — the government's authority to restrict access to a communications channel turns substantially on whether that channel has been designated as a public forum. A government email system that has never been formally declared a non-public forum is legally vulnerable to challenge when the government attempts to restrict unsolicited access to it.

HB 718 forecloses that vulnerability. It explicitly establishes, in statute, that state employee email systems are not public forums. That designation aligns Maryland with courts that have uniformly upheld similar policies in other states and gives our agencies the clearest possible legal foundation for enforcing restrictions on spam, phishing, and unsolicited bulk communications.

VI. The University System Already Lives by This Standard

One of the strongest arguments for this legislation is that Maryland's higher education institutions have already accepted its premise.

USM's IT security standards require each institution to develop acceptable use policies that address the responsible use of computing resources. The University of Maryland, College Park's policy explicitly prohibits the use of university IT resources for commercial or profitmaking purposes, or to represent the interests of outside organizations without written authorization. That is, functionally, what HB 718 codifies for state government: email systems exist for institutional purposes, not for the benefit of outside actors seeking access to those systems.

The case for consistency is simple. Institutions that employ Maryland taxpayers and deliver essential public services — whether they are state agencies or public universities — should operate under a uniform standard. Patchwork policies create uneven protection. A state agency that lacks a clear non-public-forum designation is a weaker link in Maryland's IT security chain than a university that has one. HB 718 establishes the floor that every institution should already be meeting.

VII. Addressing Anticipated Concerns

"This bill restricts the public's ability to contact government."

It does not. Marylanders retain every avenue of communication with their government: phone, mail, in-person visits, official web forms, public comment processes, public hearings, and direct contact with elected officials. What this bill restricts is the ability of commercial actors, spammers, and bad-faith senders to exploit government email systems as a vector for unsolicited mass communication. The distinction between access to government and unrestricted access to individual employee inboxes is clear, legally established, and entirely reasonable.

"DOIT's existing policies already address this."

As discussed above, they do not — not fully. The absence of a statutory definition of "state business," the absence of a non-public-forum designation, and the absence of a uniform mandate applicable to both state agencies and higher education institutions are genuine gaps. Technical spam filters address the symptom; HB 718 addresses the legal structure underlying it. Both are necessary.

"This is unnecessary regulation."

Every organization — public or private — that provides employees with work email has an acceptable use policy. Every major corporation, every law firm, every university already tells its employees that work email is for work. What is unusual is not the policy; it is that Maryland state government does not have a clear statutory basis for it. HB 718 corrects that anomaly.

VIII. Conclusion

Good government is efficient government. It is government that spends public money on public purposes, protects public infrastructure from attack, and gives public servants the legal and policy framework to do their jobs without unnecessary friction.

House Bill 718 serves all three of those goals. It stops the waste of millions of dollars in taxpayer-funded work hours. It strengthens Maryland's cybersecurity posture. And it ensures that the legal framework governing state email systems is clear, uniform, and defensible.

The bill asks nothing burdensome of anyone. It simply declares what should already be understood: Maryland's state and higher education email systems exist to serve Maryland, and they will be protected accordingly.

For these reasons, I respectfully urge the Committee to issue a favorable report on House Bill 718.