Security Industry Association
Silver Spring, Maryland

Testimony Before the Finance Committee
Maryland Senate

Opposition to Senate Bill 476

Drake Jamali
SIA Manager of Government Relations
March 11, 2020
Annapolis, Maryland

Chairwoman Kelley, Vice Chairman Jennings and members of the Committee, thank you for this opportunity to speak with you today. The Security Industry Association (SIA) is a nonprofit trade association representing businesses that provide a broad range of security products for government, commercial and residential users, including over 20 businesses with headquarters, employees and operations in Maryland.

Our members include many of the leading developers of facial recognition as well as those incorporating it into a variety of security and public safety applications. We believe transparency should be the foundation that governs it's use, and we are pleased that rather than blanket restrictions, this bill focuses on specific transparency and accountability requirements.

Facial recognition is providing enormous benefits in the commercial space, allowing individuals to securely and conveniently prove their identity to enter a venue, board a plane, perform online transactions, and access personalized experiences. It is also enabling businesses to better secure their employees, customers and property against the threat of violence, theft or other harm.

We have four specific concerns that if left unaddressed could curtail – versus sensibly regulate – beneficial uses of the technology in the state.

Frist, while the bill provides a safety and security use exception from the opt-in consent requirement, it is constructed far too narrowly. The prior requirement of suspicion of criminal activity would constrain the ability of businesses to address many safety/security risks. There are other situations impacting safety and security that either do not involve criminal activity or the suspicious activity doesn't rise to that level prior to an event unfolding.

Second, the definition of ongoing surveillance is very vague, and the restrictions around

it appears to prohibit non law enforcement uses in systems used to protect state or local government facilities, including schools, courthouses and other public buildings. In these cases, security staff can be alerted to the presence of known individuals that are potentially dangerous, but the situation may not yet rise to the level of an emergency or where law enforcement should be involved. Such individuals could enter a premises multiple times or move throughout areas covered by video surveillance, potentially triggering the "ongoing surveillance" definition. Requiring a law enforcement purpose appears to take the technology off the table for these types of uses, which can positively impact the day to day safety and security of government personnel and members of the public visiting buildings and other government facilities.

Lastly, the requirement to provide an application programming interface (API) for the third-party testing could provide and unfair advantage to larger companies using software as a service business models – which may make free or trial versions publicly available.

This requirement into law could disadvantage small U.S. developers of facial recognition designed for government use, most of which have not made their technology publicly available in order t to ensure it is only used for specific purposes. These developers should have the alternative option of participating in the National Institute of Standards and Technology (NIST) Facial Recognition Vendor Test (FRVT) program in order to meet this requirement. FRVT is the global gold standard for scientific, independent evaluations of facial recognition algorithm performance, including comprehensive measurements of differences across demographic groups. This program run by the federal government is available to developers at no cost.

We are concerned that without these improvements, the bill as drafted will have a chilling effect on the adoption of the technology, leaving Marylanders with fewer of the benefits it provides, especially for safety and security enhancements. We urge the committee to continue thoughtful consideration of these issues and work with stakeholders before moving this bill forward. Sensible privacy protections can help ensure responsible use of this technology without unreasonably restricting tools that are essential to public safety.