American Association for Laboratory Accreditation

A2LA

**March 3, 2023** **Written Testimony Supporting with Amendment – Senate Bill 0868**

On behalf of the American Association for Laboratory Accreditation (A2LA), I write regarding Maryland Senate Bill 0868 specifically as it pertains cybersecurity standards and inspection requirements.

We first wish to thank the sponsor of this bill for introducing legislation that will improve cybersecurity within the state of Maryland as well as the Senate Education, Energy, and the Environment Committee for deliberating on the proposed legislation.

By way of background, A2LA is a non-profit, accreditation body that has been based in Maryland for our forty-five-year history. We have a global presence and provide accreditation services to over 4000 actively accredited certificates representing all 50 states including 80 organizations accredited here in Maryland. We have been granting accreditation in various industries since 1979.

The criteria forming the basis for our cybersecurity inspection accreditation program is ISO/IEC 17020 Conformity Assessment - Requirements for the operation of various types of bodies performing inspections. We ourselves, as an accreditation body, have been evaluated against rigorous standards in providing this accreditation service and are recognized globally as meeting the requirements of ISO/IEC 17011. Specific to the cybersecurity industry, A2LA is the sole sourced provider of accreditation to third party assessment organizations (3PAOs) seeking Federal Risk and Authorization Management Program (FedRAMP) approval.

When establishing cybersecurity requirements for Maryland, it is important to utilize well established industry standards and procedures to qualify cybersecurity organizations. A current example of industry and government working together on a cybersecurity program is the federal program known as FedRAMP.

> **As stated on the FedRAMP website:**
>
> *FedRAMP is a unique government program that is at the epicenter of cloud technology, cybersecurity, and risk management. FedRAMP provides a standardized framework to security assessment, authorization, and continuous monitoring for cloud products and services. This framework uses a "do once, use many times" approach that saves an estimated 30-40% of government authorization costs, by reducing both time and staff required to conduct Agency security assessments. FedRAMP maintains a Marketplace of all vendors that hold a FedRAMP designation, as well as a Secure Repository for all of the authorization packages for FedRAMP Authorized vendors. FedRAMP relies on accreditation to ISO/IEC 17020 for the qualification of Third-Party Assessment Organizations (3PAOs). The 3PAOs conduct assessments of cloud service providers responsible for hosting government data. It is a successful, risk-based approach for the adoption and use of cloud services by the federal government.*

Senate Bill 0868 requires standards and criteria to be in place but does not provide for any formal qualifications to ensure that these standards are in place and adopted by organizations, resulting in a gap in security. We recommend regulations that require standards that includes qualifying cyber inspection organizations by using an existing framework based on the use of ISO/IEC 17020 accreditation provided by an International Laboratory Accreditation Cooperation (ILAC) recognized accreditation body. ISO/IEC 17020 provides the baseline inspection requirements that can be augmented with the technical requirements such as the NIST Cybersecurity Framework, NIST 800-53 and NIST SP 800-171. Three Maryland based inspection organizations hold this accreditation today and fourteen maintain this accreditation in the nation.

We recommend removing ISO 27001 because it is a management system standard and does not attest to the technical competency of an organization on its own, and therefore should not be considered as a standalone standard.

We kindly offer suggestions in **bold** and strikeouts for consideration specific to the needs of Maryland as provided in the language within SB 0868.

3.5–2A–04.

(b) The Office shall: (11) develop and maintain information technology security policy, standards, **cybersecurity organization qualifications,** and guidance documents, consistent with A WIDELY RECOGNIZED SECURITY STANDARD, INCLUDING **ISO/IEC 17020 accreditation offered by an International Laboratory Accreditation Cooperation (ILAC) signatory accreditation body** and:

(I) National Institute of Standards and Technology (NIST) CYBERSECURITY FRAMEWORK, NIST 800–53, ~~OR INTERNATIONAL ORGANIZATION FOR STANDARDIZATION (ISO) ISO 27001~~; OR

(II) IN THE CASE OF ORGANIZATIONS HANDLING CONTROLLED UNCLASSIFIED INFORMATION, NIST SP 800–171 OR THE CYBERSECURITY MATURITY MODEL CERTIFICATION FROM THE U.S. DEPARTMENT OF DEFENSE;

ISO/IEC 17020 accreditation ensures that assessment organizations are:

- impartial and independent;
- have the necessary industry accepted professional judgment and cybersecurity expertise;
- use appropriate inspection methods and procedures; and
- maintain procedures for hiring and monitoring personnel for appropriate technical knowledge, skills and experience relevant to the specific inspection.

With accreditation, governmental resources are available to focus on oversight and enforcement of the program while relying on approved, qualified technical experts for inspections.

We would be pleased to provide more background and elaborate on our comments at your convenience. If interested, please contact me via email at rquerry@A2LA.org.

Sincerely,

Randall Querry
Director of Government Relations, A2LA