February 12, 2018
Subject: Feedback on the DOC/DHS Draft Report on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure

A2LA has the following comments on the document:

As an independent third-party accreditation body, A2LA has reviewed the proposed draft report and we feel that ISO/IEC 17065, the international Product Certification conformity assessment standard, would be the most appropriate standard to implement to help achieve the goals set forth in the Draft Report. ISO/IEC 17065 is the paramount conformity assessment standard/scheme in the overall conformity assessment world, and can incorporate parts or entireties of other conformity assessment standards such as management system audits (e.g. ISO 9001 and 27001), testing (ISO/IEC 17025), personnel certification (ISO/IEC 17024) and inspections (ISO/IEC 17020) to name a few.

The strength in this standard versus many of the others mentioned above is that it requires a third-party attestation to the conformity of actual items coming out of a manufacturing/coding/controls implementation area, rather than simply the system supporting it. Utilizing a management-system-audit only approach typically fails to incorporate a verification of the actual product being produced (be it a hardware such as an IOT appliance, edge device, or enterprise grade router, or a software suite such as anti-malware application or firewall), or the system being offered or implemented in a business setting. Testing alone also leaves weaknesses from the perspective of a wide-net security approach, in that the testing under ISO/IEC 17025 will generate information about the product in question but only at one point in time. Inspection, under ISO/IEC 17020, can garner critical information about installation and/or implementation of a system (hardware and/or software configurations at a specific locale), with the possible inclusion of testing results, but can also fail to incorporate ongoing reviews.

We believe an ISO/IEC 17065 based Product Certification Scheme should be introduced and encouraged with the appropriate stakeholders involved to judge all the various impact points from both consumer and enterprise perspectives. Specifications for hardware and software security and access (e.g. mandating default passwords be changed prior to any installation or interfacing of residential/commercial grade devices, or two-factor-authentication (2FA) being mandatory in enterprise settings) should be defined, and updated at least yearly.

Continual checks of previously certified products and systems are also critical parts of an effective system. The ISO/IEC 17065 standard calls this process “Surveillance” and, just as with the initial process to certify the item in question, can involve any combination of activities to generate information about the conformity of the product or service to the ongoing security requirements.

Without a set of requirements that connected products and/or security control systems must conform to and be consistently checked against, there is little value to creating such a program.

With a new certification program, one area of concern that should be considered is the need to ensure that there is either only a single recognized program (typically recognized by government or consensus among industry), or that there is a third-party willing to attest to the equivalence of multiple schemes in the event various certification schemes crop up to respond to the needs of this industry.

A2LA, as an accreditation body, is generally not permitted to judge the value or equivalence of schemes; our role is to assess to proper performance of evaluations and decisions and surveillance tasks as defined by the certification program. It would be up to a different independent third party (for example, an industry group of security professionals, regulatory agency representatives, and manufacturing / programming corporations) to evaluate and pass judgement on the veracity and validity of any proposed certification requirements.

One final aspect that must be addressed is education of the end user pool. The government will need to support a very strong consumer and industry education program on the scheme(s) which are adopted. A good example, worth looking at, is the EPA ENERGY STAR® program. At its original onset in the 1990s, ENERGY STAR required years and a fair investment of money until the general consumer realized its benefits - and this was for a voluntary certification scheme! When mandating new requirements for security of devices and software which will inherently raise the end user costs, justification (a cost-benefit analysis) will need to be made available explaining why costs are rising.

Explanations of the impact of cyber security breaches to the individual citizen, family, and small and large businesses, along with details of the security measures being implemented and how they are designed to mitigate those impacts, can go a long way towards acceptance of the increase in prices.

Further considerations of other "carrots" to encourage rapid adoption of newly certified devices, systems, and practices should also be carried out at the policy level. For example, minor tax breaks (similar to those offered for energy efficiency improvements made by home owners) could be considered on both the individual and corporate levels, beyond any existing deductions/write-offs. Additionally, corporations which do not currently follow the Federal Risk and Authorization Management Program (FedRAMP) requirements for cyber security could voluntarily undergo a security system audit which mirrors the rigor that Cloud Services Providers are mandated to go through to keep federal business. This process, if utilized by a corporation for added assurance, could be aided by benefits such as reduced taxes or insurance rates, or be eligible for other incentives.

Ultimately, creation and maintenance of a robust certification scheme, coupled with the education of the marketplace, is the most critical and beneficial task that the agencies can invest time and money in.

We thank you for your time and invitation to comment on this Draft Report.