Response to NIST RFI

Developing a Framework to Improve Critical Infrastructure Cybersecurity

Submitted By:

The American Association for Laboratory Accreditation (A2LA)

April 8, 2013

Samantha Dizor Carter
Senior Accreditation Officer
sdizor@a2la.org

Introduction:

Conformity assessment and voluntary consensus standards play an important role in critical infrastructure for cybersecurity and should continue to play an important role as the cybersecurity framework is developed. Conformity assessment provides a number of benefits for U. S. Government Agencies and Organizations, State Regulators and/or Public Utility Commissions, Industry and Industry Associations, and Non-Profits and other Non-Government Organizations. These benefits include cost savings, lowered barriers for internal trade, a greater confidence in the accuracy of the information provided, and efficiency in the system.

There is a cost savings when utilizing existing voluntary consensus standards as time and money does not have to be spent in creation of a new conformity assessment standard. There are additional cost savings to the end users, both from the Government and Industry, as these end users don't have to perform an assessment of the cybersecurity organization or qualify them as an approved vendor in some other fashion; being accredited can immediately make them an approved vendor. Finally the cybersecurity organization benefits from a cost savings as they do not have to carry multiple recognitions in order to bid for different projects.

Utilizing already developed conformity assessment standards is also in keeping with the "National Technology Transfer and Advancement Act of 1995", Pub. L. 104-113 and the OMB Circular A-119. This Act requires federal agencies and organizations to utilize voluntary consensus standards when practical.

Conformity assessment through recognized Accreditation Bodies also lowers barriers for internal trade as these Accreditation Bodies are already recognized internationally. Therefore, the cybersecurity organizations that are accredited by recognized Accreditation Bodies would benefit from the internal recognition and would not need separate accreditations in order to perform work internationally.

There is a greater confidence in the accuracy of the work of a recognized cybersecurity organization as their processes will have been reviewed by an accreditation organization. Part of the accreditation process is not just looking at the organizations management system but also looking at their technical expertise and technical processes. An independent third party review of these process ensures that the organization is in conformance to the guidelines that will be established with the cybersecurity framework and also ensures that the organization has the technical expertise to perform the job that they are hired to do.

Using a recognized Accreditation Body to accredit to a voluntary consensus standard already developed builds efficiency into the system. As the standard is already developed and the Accreditation Bodies already exists there is no need to spend time creating a new voluntary consensus standard. There is additional efficiency from being able to use one accreditation to market to multiple international markets and various Government and Industry companies nationally. Finally, there is efficiency for the end user as approving the vendor is as simple as requesting evidence that they have been accredited by a recognized Accreditation Body.

Current Industry Approach:

The conformity assessment approach is not new to the cybersecurity industry. FedRAMP has been a successful conformity assessment program and is poised to switch over to private Accreditation Bodies to administer the program. Other successful programs include accreditation for companies testing Gaming Systems (i.e. slot machines and/or internet gaming) and Interoperability testing for IPv6.

As the cybersecurity framework is developed the question should not be whether or not to use internal standards to assess organizations providing cybersecurity products but which standards will benefit this industry the most. Of the many international standards for conformity assessment bodies there are three would be of benefit for the cybersecurity organizations. They are ISO/IEC 17065:2012 Conformity assessment - Requirements for bodies certifying products, processes and services, ISO/IEC 17020:2012 Conformity assessment - Requirements for the operation of various types of bodies performing inspection, and ISO/IEC 17025:2005 General requirements for the competence of testing and calibration laboratories. All of these standards should play a role in our nation's cybersecurity framework.

ISO/IEC 17065:2012 pertains to organizations that certify products, processes and services. These organizations would certify a cybersecurity company's specific product, process and/or service that could then be sold to an end user (i.e. a U. S. Government Agency or Industry). This standard is currently utilized in the Gaming Industry to certify certain products (i.e. slot machines); this could be used in the cybersecurity industry to certify that a service provided by a company is secure.

ISO/IEC 17020:2012 is for Inspection Bodies and has already been utilized by the FedRAMP program. This program has been successful and is being transferred over to third party accreditation organizations that are ILC MRA signatories.

ISO/IEC 17025:2005 provides for the accreditation of testing laboratories that would test to the protocol developed during the development of the cybersecurity framework. These testing laboratories would provide an important foundation for the cybersecurity framework as these laboratories will provide the testing results necessary to perform certain inspections and certify products.

The Role of Accreditation Bodies:

Finally, the adoption of conformity assessment standards should include requirements to use accreditation bodies that are signatories of the ILAC MRA (International Laboratory Accreditation Cooperation (ILAC) Mutual Recognition Arrangement (MRA). Each accreditation body that is a signatory to the ILAC MRA commits to:

- Maintaining conformity with the current version of ISO/IEC *17011 Conformity Assessment – General Requirements for bodies providing assessment and accreditation of conformity assessment bodies* and supplementary documents.

- Ensuring that all organizations that are accredited comply with appropriate conformity assessment standard

The ILAC MRA has been structured to build on existing and developing regional MRAs established around the world. Regional cooperation bodies that operate a regional MRA, coordinate peer evaluations and thereby maintain confidence in the accreditation bodies that are signatories to the regional MRA.

Currently, the European cooperation for Accreditation (EA), the Asia Pacific Laboratory Accreditation Cooperation (APLAC) and the Inter-American Accreditation Cooperation (IAAC) are the only ILAC recognized regional cooperation bodies. This means that the MRA process and evaluation procedures of EA, APLAC and IAAC have been peer evaluated by ILAC and have been deemed to meet ILAC requirements. Recognized regional cooperation bodies are re-evaluated on an on-going basis, over a 4 year period, i.e. all aspects of the regional cooperation body's operation must be evaluated at least once every 4 years. A2LA is a signatory to the MRAs of APLAC and IAAC.

In Conclusion:

Conformity Assessment is the approach to take when developing the cybersecurity framework. Use of Accreditation Bodies to assess organizations to conformity assessment standards provides:

- Cost savings:
  - to any organization that uses accredited cybersecurity organizations as they will not have to assess the cybersecurity organization themselves.
  - to regulators and government organizations as they will not have to create their own conformity assessment process.
  - to the cybersecurity organization as they will only need one accreditation to perform work for a variety of government, industry, and other organizations here in the United States as well as internally.
- Ensures greater accuracy and reliability of the services provided by the cybersecurity organizations.
- Lowered barriers to international trade as these are internationally accepted standards.
- Efficiency in the system as one accreditation can be used nationally and internationally for all types of organizations.