May 25, 2021

ANSI National Accreditation Board Comments
Workshop on Standards and Guidelines to Enhance Software Supply Chain Security

Initial list of secure software development lifecycle standards, best practices, and other guidelines acceptable for the development of software for purchase by the federal government.

Needs for Conformity Assessment [Accreditation]

The ANSI National Accreditation Board (ANAB) is a non-governmental organization that provides accreditation services and training to public- and private-sector organizations, serving the global marketplace. ANAB is the largest accreditation body in North America and provides services in more than 75 countries.

Conformity assessment is defined as a "demonstration that specified requirements relating to a product, process, system, person or body are fulfilled." The activities applied in today's marketplace include certification, inspection, registration, supplier's declaration, testing, and the one dimension in which ANAB is directly engaged: accreditation.

Ultimately, the marketplace and customers of conformity assessment services measure the beneficial value of accreditation. For most suppliers, the primary benefit of accredited third-party certification is to meet a purchaser's or regulator's requirement for this independent evaluation of compliance. Increasingly, suppliers' procurement organizations are specifying and government agencies are recognizing accredited, third-party certification as an optional dimension of their systems for risk management.

ISO/IEC 27001 Information Security Management System, ISO/IEC 27001 provides a model for establishing, implementing, operating, monitoring, reviewing, maintaining and improving an information security management system (ISMS). The design and implementation of an ISMS is influenced by the organization's needs and objectives, security requirements, processes, size, and structure.

Product Certification, ANAB provides accreditation in accordance with ISO/IEC 17065 for product, process, and service certification programs to ensure that the marketplace can gain confidence for their activities.

Laboratory Accreditation, ANAB provides accreditation to ISO 17025 for laboratory testing to multiple standards in many industry-specific programs.

The U.S. government increasingly relies on ANAB accreditation for the verification of the quality of certification programs. In view of the numerous certification programs and the necessity to assist the consumer in making informed decisions, government entities look to ANAB to provide accreditation programs that improve industry practices and distinguish quality certification programs.

ANAB conducted a survey in 2020 to help determine the need for accreditation of Cybersecurity testing and

certification schemes. Recommendations from the survey are as follows:

- Set up an industry advisory group on cybersecurity conformity assessment to provide guidance, and alleviate widespread confusion in the marketplace;
- Provide educational opportunities to reduce misunderstanding of cybersecurity conformity assessment approaches and terminology – *e.g.,* accreditation vs certification, etc.;
- Support a NIST cybersecurity workshop. During an interview, NIST itself opined that a cybersecurity workshop would be timely and indicated their willingness to sponsor it; and.
- Form an ANAB Accreditation Committee Task Force to assist in establishing an ANAB accreditation program for cybersecurity schemes.

ANAB is in the process of acting on these recommendations and is forming a task force that will be responsible to review the trends on conformity assessment related to cybersecurity and support ANAB on the design of a robust accreditation program based on the ISO/IEC 17065 and the good practices in this sector.

Executive Order on Improving Cybersecurity of the Federal Government

Per item 2 in NIST Workshop invitation - *Initial list of secure software development lifecycle standards, best practices, and other guidelines acceptable for the development of software for purchase by the federal government*. *This list of standards shall include criteria and required information for attestation of conformity by developers and suppliers.*

The following elements and standards should be considered as best practices and guidelines for use in the development of conformity assessment criteria used for the purchase of software by the federal government:

- **Schemes.** Development of certification/testing schemes used to determine the methods as noted in the Executive Order: " 4(e)(ix) attesting to conformity with secure software development practices; and (x) ensuring and attesting, to the extent practicable, to the integrity and provenance of open source software used within any portion of a product;"
- **Standards.** Identify industry standards for use in the evaluation (testing) of software used in any portion of a product;
- **Testing.** Evaluation (testing) of products to ensure compliance with the applicable cybersecurity standards;
- **Certification.** Certification bodies perform evaluation of product and processes used to provide integrity of open source software used with any portion of a product; and
- **Accreditation.** Certification Bodies and Testing Laboratories accredited by recognized Accreditation Bodies to ISO/IEC 17065 and ISO/IEC 17025 respectively to support certification/testing schemes.

It is expected that the development of ANAB cybersecurity accreditation programs will support certification and testing programs resulting from the President's Executive Order on Improving the Cybersecurity of the Federal Government, issued on May 12, 2021. The ANAB conformity assessment programs will enable such certification/testing schemes to be conducted in a manner consistent with OMB Circular A-119 and NIST Special Publication 2000-02 (Conformity Assessment Considerations for Federal Agencies).

Certification bodies seeking accreditation from ANAB require expertise in the NIST 800 publication series related to cybersecurity and risk assessment. It is expected that the development of ANAB cybersecurity accreditation programs will build on existing accreditation programs (ISO/IEC 17021) and will apply new programs (ISO/IEC 17065 and 17020) as well.

ANAB is prepared to work with NIST and other agencies in providing educational opportunities to aid in a better understanding of how conformity assessment works and can benefit the development of schemes to enhance software supply chain security (pilot programs).