January 19, 2018

Submitted via e-mail to cyberframework@nist.gov

Re: Comments on the NIST Framework for Improving Critical Infrastructure Cybersecurity – v1.1 Draft 2

1. Introduction

The International Federation of Inspection Agencies ("IFIA") is pleased to provide the following comments on the NIST Framework for Improving Critical Infrastructure Cybersecurity Version 1.1 Draft 2 ("Framework").

IFIA is a trade federation that represents over 60 of the world's leading independent third-party testing, inspection and certification (TIC) companies. IFIA members offer conformity assessment services, including testing, inspection, certification, systems audits, training, technical and documentary support. These services provide global market access for manufacturers, and help ensure that not only regulatory requirements are fulfilled, but also that reliability, economic value, environmental impact and sustainability are enhanced.

IFIA applauds the National Institute of Standards and Technology (NIST) efforts to improve the Framework and approaches regarding coordination and collaboration with the private sector to strengthen cybersecurity. Advancing cybersecurity provides an ideal opportunity for a strong public-private partnership.

IFIA encourages NIST to consider the following recommendations:

- Provide an efficient route for component or product IT assurance
- Continue dialogue and sharing of views and approaches with international stakeholders so that the Framework can further its mission of providing a common language for cybersecurity risk management
- Leverage public-private partnerships in developing public policy related to cybersecurity
- Leverage third-party validation that can help mitigate safety and performance risk
- Consider the importance of conformity assessment schemes to improve cybersecurity

IFIA Americas Committee | 6718 Kenwood Forest Lane | Bethesda, MD 20815 USA | +1 240 507 3392 | ifia-federation.org

2. The TIC sector's views of the Draft Framework

IFIA commends NIST for its effort to continue improving the Framework and for NIST's commitment to an inclusive approach through ongoing consultation with stakeholders. The Framework's favorable receipt and adoption by the private sector is attributable to a number of factors, including NIST's ongoing reviews and engagement with the private sector, the Framework's risk based approach, the ability for the organizations to define the risk tolerance and the smart application of existing standards and industry practices.

We offer the following comments addressing specific language and concepts we believe should be emphasized or included in the Framework. First, in Framework Section 2.1, we believe **greater emphasis should be placed on the need to mature or develop sound categories, sub-categories and informative references across all five key functions**. Line 317 of the unmarked document makes reference to it, but more emphasis is needed.

IFIA also believes that the Framework should take the **opportunity to provide an efficient route for third party component or product IT assurance**. Unless the Framework appropriately emphasizes security assurance of underlying components, efforts and investments in improving processes could be squandered. We note that while NIAP's (the National Information Assurance Partnership of which NIST is a partner) new approach to Common Criteria has helped make evaluations more efficient, timely and cost effective, there is room for improvement especially regarding addressing areas such as real-world vulnerabilities. We encourage NIST to emphasize the basic underlying model of repeatable, testable and achievable certification but also account for the flexibility needed to apply a common set of requirements to a wide variety of products.

As NIST continues to review and modify the Framework, we encourage NIST and stakeholders to consider whether there are lessons to be learned from the approach that is taking shape with the European Commission's proposal for a Regulation establishing a "European Cybersecurity Certification Framework" for ICT products and services. Currently, there is no single cybersecurity certification scheme in place across Europe, making it difficult to accurately compare services, products, and systems. Even the certification schemes that exist in Member States are insufficient to handle the large number of products that could be certified per year. While the proposed regulation remains in draft form, we believe it could promote greater harmonization across the Single Market, thereby reducing the costs ("one-stop-shop") and time-to-market for manufacturers, by eliminating duplicative national requirements and providing greater transparency for all stakeholders involved. IFIA supports such harmonization across all the EU Member States. We recognize the inherent differences in operating in the U.S. Market, but **we encourage NIST to continue dialogue and sharing of views with both European, and other counterparts**, as NIST continues developing its Framework.

IFIA Americas Committee | 6718 Kenwood Forest Lane | Bethesda, MD 20815 USA | +1 240 507 3392 | ifia-federation.org

3. Public-Private Partnerships

IFIA members encourage the government to **leverage public-private partnerships in developing public policy related to cybersecurity** by incorporating consensus-based standards, available accreditation schemes, and globally recognized practices to meet its compliance interests. By working with the private sector, government agencies can promote transparency, leverage private sector resources, and contribute to economic and job growth.

For more than a century, IFIA member companies have worked with manufacturers, academia, and government stakeholders across the globe to build and strengthen critical infrastructure. IFIA members continue to adapt to meet the demands of an expanding and evolving concept of safety and security resulting from new digital technologies, innovations, and a more complex global marketplace. IFIA members have a shared commitment to strengthening cybersecurity. While improving cybersecurity is a shared objective for both the public and private sectors, finding common ground between the government and the private sector on how best to achieve that objective is the subject of much debate, in the United States and abroad. IFIA member companies seek to be a bridge in that debate. Grounded in science and collaboration IFIA member companies engender trust and confidence in pioneering technologies, from electricity to the internet. The result is a **third-party validation that can help mitigate safety and performance risk**. To help innovators create safer, more secure and sustainable products, IFIA members aspire to apply that science and collaboration to the challenge of cybersecurity. Whether the development of related standards, assessment programs or research partnerships with government bodies, IFIA member companies work to provide flexible, and globally relevant pathways to meet both government and private sector needs.

4. Importance of conformity assessment schemes to improve cybersecurity

Security of connected devices is a major concern for governments, manufacturers and consumers alike. There is growing awareness across multiple industries that helping ensure improved levels of cybersecurity will enable connected technologies to move forward faster and in a safer manner. IFIA members' intent is to assist governments, vendors and the public in mitigating cyber risks. IFIA encourages NIST to **consider the importance of conformity assessment schemes to improve cybersecurity.** The conformity assessment method used to demonstrate compliance should be based on risk assessment and confidence needs. Such methods can include sampling and testing, inspection, supplier's declaration of conformity, certification and management system assessment and registration. IFIA member companies' capabilities and expertise are for manufacturers looking for trusted support in assessing security risks while they continue to focus on product innovation to help build safer, more secure products, as well as for purchasers, owners, system integrators, and retrofitters who want to mitigate risks by sourcing products assessed by a trusted third party.

IFIA Americas Committee | 6718 Kenwood Forest Lane | Bethesda, MD 20815 USA | +1 240 507 3392 | ifia-federation.org

Using a combination of cybersecurity standards, evaluation, and certification will improve systems security and risk management, through metrics, measurements, and benchmarks that support acquisition requirements for connected products across their lifecycle. Conformity assessment is a reasonable and responsible model for addressing the challenges of acquisition and cybersecurity, and improving cybersecurity posture throughout the product lifecycle.

Trusted, independent third-party conformity assessment is a cost-effective policy solution as it provides the highest level of confidence and helps government leverage private-sector resources.

5. Conclusion

The NIST Framework is an invaluable tool that helps fills a gap in the need to secure cybersecurity. IFIA supports NIST's effort to continuing improving it based on stakeholder input and recommends that NIST consider providing an efficient route for component or product IT assurance, consider leveraging third-party validation and the development of conformity assessment schemes that can help mitigate safety and performance risk.

Thank you for the opportunity to offer the above comments. If you have any questions, please feel free to contact Roberta Telles at +1.240.507.3392.

Sincerely,

Roberta Telles
IFIA
Executive Director Americas
rtelles@ifia-federation.org
M: +1.240.507.3392

Hanane Taidi
IFIA
Director General
htaidi@ifia-federation.org
M: +32473629947