From: Luke Bader
Sent: Thursday, January 18, 2018 1:41 PM
To: cyberframework <cyberframework@nist.gov>
Subject: FAIR Institute and The Open Group Comments to NIST CSF v 1.1 Draft 2

Hello,

My name is Luke Bader and I am Director of Memberships and Programs at the FAIR Institute. The Institute has partnered with The Open Group to submit comments on the NIST CSF v 1.1 Draft 2 on behalf of our members.

Our comments are attached. Please contact me with any questions you may have. I look forward to hearing back and reading the final version of CSF v 1.1.

Best,

Luke

Luke Bader
Director, Memberships and Programs
The FAIR Institute

[*Attachment copied below*]

January 18, 2018

Mr. Matthew Barrett
National Institute of Standards and Technology
100 Bureau Drive, Stop 8930
Gaithersburg, MD 20899

Dear Mr. Barrett,

The FAIR Institute and The Open Group commend NIST for making the first step in terms of providing measurement criteria for assessing risk. Additionally, we would like to thank you for allowing us to submit our comments.

About the FAIR Institute

- The FAIR Institute is a rapidly growing, non-profit, expert organization that has amassed over 2,200 members in its first two years and is on track to reach 3,000 members by the end of summer 2018.
- Our members are forward-thinking risk officers, cybersecurity leaders, and business executives from enterprises of all sizes, government organizations, and academic institutions around the globe.
- A dozen universities are currently offering risk management courses based on FAIR and over thirty universities have signed up to offer courses starting in the fall of 2018. The syllabus that universities are adopting includes how FAIR can augment NIST CSF by adding an economical dimension to risk analysis.
- We operate with the central mission to establish and promote information risk management best practices that empower risk professionals to collaborate with their business partners on achieving the right balance between protecting the organization and running the business.
- Factor Analysis of Information Risk (FAIR) is the standard risk model behind our mission. FAIR is the only international standard quantitative model for information security and operational risk as chosen and published by The Open Group, a global consortium that enables the achievement of business objectives through IT standards.
- The FAIR model provides a consistent set of definitions that allows an organization to speak in the business language, prioritize risks, and defend risk decisions using an advanced risk model.

About The Open Group

- The Open Group is a global consortium that enables the achievement of business objectives through technology standards.
- Our diverse membership of more than 680 organizations includes customers, systems and solutions suppliers, tool vendors, integrators, academics, and consultants across multiple industries.

- The Open Group has published two standards based upon FAIR, these are the Risk Taxonomy Standard (O-RT, and the Risk Analysis Standard (O-RA, collectively referred to as the Open FAIR body of knowledge.

Objectives of the NIST CSF v 1.1 and of the EO 13800 related to cost-effective decision making

Our comments center on the NIST CSF v. 1.1 Draft 2 Section 4.0 on Self-Assessing Cybersecurity Risk with the Framework.

> *"The Cybersecurity Framework is designed to reduce risk by improving the management of cybersecurity risk to organizational objectives. Ideally, organizations using the Framework will be able to measure and assign values to their risk along with the cost and benefits of steps taken to reduce risk to acceptable levels. The better an organization is able to measure its risk, costs, and benefits of cybersecurity strategies and steps, the more rational, effective, and valuable its cybersecurity approach and investments will be."*

The above stated objective has been re-emphasized by the recent Executive Order 13800 by President Trump which requires government agencies to both (1) indicate the state of their cyber risk activities and (2) the cost effectiveness and return on investment of their cyber initiatives.

In recent discussions with the Office of Management and Budget (OMB), OMB representatives expressed the limitations in using the NIST CSF in its current form and proposed measurements as described in v. 1.1 to meet the Executive Order's requirements. What they are getting from agencies are volumes of anecdotal evidence related to CSF activities with no, or very limited and inconsistent, economical and budgetary considerations.

FAIR Institute and Open Group Recommendation

The market is speaking. The number of our member organizations who use NIST CSF and FAIR in tandem continues to grow every quarter. These organizations recognize the complementary nature of the NIST CSF and FAIR, as FAIR adds an economical dimension to the CSF as illustrated in a series of highly popular articles listed on both the NIST CSF Industry Solution page and the FAIR Institute website. Organizations that use NIST CSF and FAIR together are part of many critical infrastructure industries such as: financial services, defense, utilities, and technology.

The FAIR Institute and The Open Group's ultimate recommendation is to explicitly include FAIR, in the NIST CSF v 1.1, as a pragmatic method to measure cybersecurity risk and assess the effectiveness of controls and other risk management activities.

In addition, based upon member inputs, The Open Group Security Forum wrote a guide to using Open FAIR and the NIST Cybersecurity Framework. A sample list of FAIR Institute members is listed at the following link. A listing of The Open Group's membership may be found at this link.

At a minimum, listing the Open FAIR standards (O-RA and O-RA) in sections ID.RA-1 through ID.RA-6 will help critical infrastructure organizations to more effectively measure risk.

We believe that failure to include this standard methodology for quantifying risk that is widely adopted, will set the industry back by keeping it anchored to risk measurement methods, such as ordinal scales (currently proposed in draft v 1.1), which have proven to be highly subjective and imprecise and that do not allow effective decision making related to prioritizing risk activities and optimizing investment dollars.

The inclusion of the FAIR model as a standard measurement method in CSF v 1.1 would help enterprises and government organizations at large to adopt proven and state-of-the-art quantification practices that many of their peers are already adopting.

We would like to reiterate that the FAIR model is an open international standard by The Open Group, a global standards consortium that includes numerous government organizations as well as many organizations from critical infrastructure industries as its members. The FAIR principles have been captured and published in standards documents that are available free of charge to any interested party. This adoption of FAIR by a standards body should address the concern previously brought to us by NIST representatives as being an expression of a specific commercial entity. We would be happy to share more details if that is of interest.

The FAIR Institute and The Open Group would be available to support NIST in the effort of integrating the FAIR model in a new draft in any way possible.

Sincerely,

Luke Bader
Director
The FAIR Institute

Jim Hietala
Vice President
The Open Group