April 5, 2013

Diane Honeycutt

National Institute of Standards and Technology

100 Bureau Drive, Stop 8930

Gaithersburg, MD 20899

Dear Ms. Honeycutt,

In response to the Request for Information (RFI) from the National Institute of Standards and Technology (NIST), regarding the CyberSecurity Framework, The Open Group respectfully submits these comments on behalf of The Open Group Security Forum.

Sincerely,

Jim Hietala

VP, Security

The Open Group

---

Open Group Comments:

In response to the Request for Information (RFI) from the National Institute of Standards and Technology (NIST), regarding the CyberSecurity Framework, The Open Group respectfully submits these comments on behalf of The Open Group Security Forum.

The Open Group Security Forum noticed a number of areas mentioned in the RFI printed in the Federal Register where existing standards published by The Open Group are directly relevant to NIST and the US Federal Government, in developing the CyberSecurity Framework. These include (among many others) objectives in the following areas:

1. Developing a framework including standards methodologies, procedures and processes that align policy, business, and technological approaches to address cyber risks
2. Providing the mechanisms for owners and operators of critical infrastructure to identify, assess, and manage cybersecurity-related risk
3. Metrics, methods, and procedures that can be used to assess and monitor, on an ongoing or continuous basis, the effectiveness of security controls that are selected and deployed
4. A comprehensive risk management approach

A number of standards developed and published by The Open Group members, through our open consensus process, relate directly to these objectives. These are described below.

1. O-ISM3 Standard, Information Security Management System. Relating to objective 1 above, O-ISM3 provides a security program management methodology that allows for relating business objectives to security controls, such that security requirements and controls flow from business and organizational goals and objectives. A key distinguishing feature is that each business control provides metrics on how well it is achieving its assigned security target. O-ISM3 is compatible for use with ISO/IEC 27001, COBIT, and ITIL standards. An associated Guide - Optimizing ISO/IEC 27001 using O-ISM3 - explains how to use O-ISM3 to produce performance metrics from ISO/IEC 27001
2. Regarding the identification and measurement of risk, and developing a comprehensive risk management approach (objectives 2 and 4 above), The Open Group has a number of risk best practices publications and standards to recommend.
    a. Risk Taxonomy Standard. This standard is based upon FAIR, Factor Analysis for Information Risk. FAIR is the leading quantitative risk analysis methodology, having been widely adopted by large enterprises. The Open Group standardized the taxonomy from FAIR.
    b. Technical Guide: Requirements for Risk Assessment Methodologies. This guide provides best practices guidance for those performing risk analysis.

c. Technical Guide: FAIR – ISO/IEC 27005 Cookbook. This guide shows how to use the FAIR risk analysis methodology in support of ISO27005 risk management programs.
d. The Open Group is also developing, and will be launching in July, 2013, a risk analyst certification program based upon FAIR.
e. Dependency Modeling Standard (O-DM). In our increasingly collaborative business world, this standard performs risk assessments for an organization's dependencies on external factors, by modeling its operations and applying metrics to assess and manage their resilience to operational failure. Published in 2012, it has already achieved significant adoption by large enterprises.

3. In support of ongoing and continuous management of security controls (objective 3 above), there are two standards from The Open Group that we commend to your attention:.
    a. The aforementioned O-ISM3 standard, which delivers metrics for security controls, and a framework for continuous improvement.
    b. Automated Security Compliance (O-ACEML). This standard defines a high-level front end to set security configuration requirements for IT systems, and then monitors that the system stays in compliance to that configuration, raising alerts if it falls out of compliance. This is part of our Open Group Security Automation work program using SCAP.