April 8, 2013

From: Sally Long, The Open Group, Forum Director - on behalf of The Open Group Trusted Technology Forum

Subject: The Open Trusted Technology Provider Standard – Mitigating Maliciously Tainted and Counterfeit Products (O-TTPS) Version 1.0

To: NIST, Cybersecurity Framework Team (Developing a Framework to Improve Critical Infrastructure Cybersecurity)

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 Trusted Technology Forum (OTTF).

The OTTF has just released a new international standard, *The Open Trusted Technology Provider Standard – Mitigating Maliciously Tainted and Counterfeit Products (O-TTPS) V1.0*, which is available at the following link: http://www.opengroup.org/bookstore/catalog/c139.htm

Additionally, the OTTF will have an accreditation program to assess conformance to the Standard. Membership in The Open Group is not required to access or adopt the Standard, which is freely available. Accreditation can be pursued by technology providers and suppliers, large and small, as well as integrators.

Consistent with the information on the Federal Register, the Standard will address many of the desired attributes expressed below:

> "Given the diversity of sectors in critical infrastructure, the Framework development process is designed to initially identify cross-sector security standards and guidelines that are immediately applicable or likely to be applicable to critical infrastructure, to increase visibility and adoption of those standards and guidelines…"

The new standard is derived from industry best practices to mitigate maliciously tainted and counterfeit Commercial Off The Shelf (COTS) Information and Communication Technology (ICT). Further, it is:

- risk based,
- outcome based,
- measureable, and
- applicable across all critical infrastructure sectors.

This global Standard was developed by the members, and approved through The Open Group Standards process. The members of the OTTF include: industry organizations from multiple countries, government related organizations and third party certification laboratories, demonstrating the effectiveness of working together and building consensus standards through public/private partnership.

The standard is based on providers' product life cycles and is accompanied by a conformance/accreditation program. These provider practices are divided into two basic categories of product life cycle activities: Technology Development and Supply Chain Security.

Specifically, V1.0 addresses:

- Product Development/Engineering Requirements in:
    - Software/Firmware/Hardware Design Process
    - Development/Engineering Process and Practices
    - Configuration Management
    - Quality/Test Management
    - Product Sustainment Management

- Secure Development/Engineering Requirements in:
    - Threat Analysis and Mitigation
    - Run-time Protection Techniques
    - Vulnerability Analysis and Response
    - Product Patching and Remediation
    - Secure Engineering Practices
    - Monitor and assess the impact of changes in the threat landscape.

- Supply Chain Security Requirements In:
    - Risk Management
    - Physical Security
    - Access Controls
    - Employee and Supplier Security
    - Business Partner Security
    - Supply Chain Security Training
    - Information Systems Security
    - Trusted Technology Components
    - Secure Transmission and Handling
    - Open Source Handling
    - Counterfeit Mitigation
    - Malware Detection

The Open Group has liaisons with ISO/IEC JTC1 27 WG3 and WG4 to harmonize their work. The scope of this standard covers COTS ICT as it pertains to IT Security and the mitigation of maliciously tainted and counterfeit products. It is important to stay in alignment because we are representing the COTS ICT community around supplier relationships within supply chains.

The O-TTPS and its accreditation program is being developed by consensus under The Open Group by the members of the OTTF.. The accreditation program is in the piloting stage, with a public launch of the program planned for the Nov-Dec 2013 timeframe.

The Open Group currently has more than 30,000 individuals, representing more than 430 member enterprises, from all sectors of the industry in more than 90 countries.

About The Open Group

The Open Group is an international vendor- and technology-neutral consortium upon which organizations rely to lead the development of IT standards and certifications, and to provide them with access to key industry peers, suppliers and best practices. The Open Group provides guidance and an open environment in order to ensure interoperability and vendor neutrality. Further information on The Open Group can be found at http://www.opengroup.org.