Executive Summary of
The Open Group's testimony to the House Energy and Commerce Oversight and Investigations Subcommittee Hearing on
IT Supply Chain Security: Review of Government and Industry Efforts

The Open Group is a global consortium that enables the achievement of business objectives through IT standards. We will present the work undertaken by The Open Group Trusted Technology Forum (OTTF) to address a clear cybersecurity challenge in the shared, multi-stakeholder risk environment of the global supply chain.

The OTTF is developing the Open-Trusted Technology Provider Standard to provide organizational commercial best practices that, when properly adhered to, will enhance the security of the global supply chain and the integrity of COTS ICT products throughout the entirety of the product life cycle; through design, sourcing, build, fulfillment, distribution, sustainment, and disposal phases. By adopting the Standard, and by committing to conform to these best practices, technology providers, hardware and software component suppliers and integrators of all sizes, will help assure the integrity of their COTS ICT products. Organizations that demonstrate their conformance through a planned accreditation program will be considered a certified Trusted Technology Provider that "builds with integrity", allowing customers to "buy with confidence".

STATEMENT of

David Lounsbury, Chief Technology Officer, The Open Group on behalf of The Open Group and The Open Group Trusted Technology Forum

Submitted for the record

House Energy and Commerce Oversight and Investigations Subcommittee Hearing on

IT Supply Chain Security: Review of Government and Industry Efforts

March 27, 2012

Chairman Upton, Ranking Member Waxman and distinguished members of the Committee:

On behalf of The Open Group and the Open Group Trusted Technology Forum, I am pleased to submit the following statement for the record of the hearing entitled: IT Supply Chain Security: Review of Government and Industry Efforts, held on March 27, 2012. The Open Group was invited to discuss The Open Group Trusted Technology Forum's plans to address some of the challenges in securing the global supply chain.

The Open Group

The Open Group is a global consortium that enables the achievement of business objectives through IT standards. With more than 400 member organizations, The Open Group has a diverse membership that spans all sectors of the IT community;

customers, systems and solutions suppliers, tool vendors, integrators, and consultants, as well as academics and researchers. The Open Group staff works with our members and other constituencies in order to:

- Capture, understand, and address current and emerging requirements, and establish policies and share best practices
- Facilitate interoperability, develop consensus, and evolve and integrate specifications and open source technologies
- Offer a comprehensive set of services to enhance the operational efficiency of consortia
- Operate the industry's premier certification service

The Open Group Trusted Technology Forum (OTTF)

The Open Group Trusted Technology Forum, a forum of The Open Group, is a global initiative that invites industry, government, and other interested participants to work together to evolve the Open-Trusted Technology Provider Standard (the Standard), currently published as a "snapshot", which is a draft version of what is intended to become a final open standard. The snapshot provides organizational commercial best practices that, when properly adhered to, will enhance the security of the global supply chain and the integrity of Commercial Off –the- Shelf (COTS) Information and Communication Technology (ICT) products. It provides a set of guidelines and best practice requirements and recommendations that help assure against tainted and counterfeit products (discussed below) throughout the entirety

of the COTS ICT product life cycle; through design, sourcing, build, fulfillment, distribution, sustainment, and disposal phases.

The snapshot was released on March 9, 2012 and is intended to become an Open Trusted Technology Provider Standard, after evaluating initial feedback on the snapshot, developing conformance criteria to demonstrate adherence, and defining an accreditation program. The snapshot and the subsequent published versions of the Standard are open standards and can be downloaded free of charge from The Open Group's website to help assure broad adoption globally.

Given the fast-moving pace of change in technology and the risk landscape, The Open Group Trusted Technology Forum (OTTF or "The Forum") plans to take a dynamic and phased approach, staging additional standards over time. As threats change or market needs evolve, the Forum intends to update the Standard by releasing addenda to address new specific threats or market needs.

The Open Trusted Technology Forum is a government-industry partnership.

The Forum is an effective example of a cooperative, public/private partnership working effectively to address a clear cybersecurity challenge in a shared, multi-stakeholder risk environment, such as the global supply chain. The Forum was initiated through informal discussions organized by The Open Group between government and industry where the then current Undersecretary for Department of Defense (DoD)/Acquisition Technology & Logistics (AT&L) posed the following question: "How can the DoD safely procure IT technology from an increasingly global supply chain?" The discussions focused on the challenges associated with an

increased reliance on the use of COTS ICT products in commercial enterprises and governments, including the defense industry, challenges compounded by the fact that these products rely on a sometimes unpredictable supply chain in a rapidly-changing threat environment.

The parties involved in the early discussions then formalized an initiative under The Open Group as the Open Group Trusted Technology Forum. The Forum member organizations currently are: Apex Assurance, atsec Information Security, Boeing, Booz Allen Hamilton, CA Technologies, Carnegie Mellon University Software Engineering Institute (SEI), Cisco, EMC, Fraunhofer SIT, Hewlett-Packard, IBM, IDA, Juniper Networks, Shenzhen Kingdee Middleware, Lockheed Martin, MITRE, Microsoft, Motorola Solutions, NASA, Oracle, Office of the Under Secretary of Defense for Acquisition, Technology and Logistics (OUSD AT&L), SAIC, Tata Consultancy Services, and the U.S. Department of Defense/CIO.

The Forum participants recognize the value the Standard can bring to governments and commercial customers worldwide, particularly since the Standard itself is informed by the practical experience and knowledge of a wide range of individuals from customer, vendor and other organizations. Customer organizations can incorporate consideration of this standard into their sourcing and procurement strategies, as appropriate.

The recent release of the snapshot of the Standard allows:

- acquirers and customers to begin consideration of how this standard fits into their procurement and sourcing strategies, and to consider recommending

the adoption of the best practice requirements to their providers and integrators.

- providers, component suppliers, and integrators to begin planning for the eventual implementation of the Standard in their organizations

The Standard is aimed at enhancing the security of the global supply chain

Adopting best practices that have been taken from the experience of mature industry providers, rigorously reviewed through a consensus process, and established as requirements and recommendations in the Standard will provide significant advantage in helping reduce risk. By adopting this Standard, and by committing to conform to these best practices, technology providers, large and small, hardware and software component suppliers and integrators, will help assure the integrity of their COTS ICT products. This Standard is sufficiently detailed and prescriptive to be useful in raising the bar for all providers and lends itself to an accreditation process to provide assurance that it is being followed in a meaningful and repeatable manner.

The initial version of the Standard addresses two types of risks inherent in the acquisition and use of COTS ICT products:

- Tainted product risk – a product is produced by the provider and is acquired through reputable channels, but has been tampered with maliciously.

- Counterfeit product risk – a product is produced other than by, or for, the provider, or is supplied by other than a reputable channel, and is presented as being legitimate.

The Forum takes a comprehensive view about the best practices a provider should follow. The Standard specifies practices that providers can incorporate in their own internal product life cycle processes, i.e. that portion of product development that is "in-house" and over which they have relatively direct operational control. Additionally, the Standard describes supply chain security practices that should be followed when a provider is incorporating third-party hardware or software components, or when depending on external manufacturing and delivery or supportive services.

The value of this approach is that it is process-focused, and thus will be horizontally integrated into a company's business processes. While there may be existing standards in the industry that have requirements for designing and implementing security driven functionality and where there is corresponding evaluation on a per product version basis, this Standard is intended to provide a broader perspective, with assurances that products have not been tainted or corrupted with counterfeit components while being developed or manufactured in the global supply chain. So although a product version may pass an evaluation – what happens in the development and production of that product is a different scenario and one that the Forum is addressing in the Standard.

Conformance Criteria and Accreditation

The Forum is in the process of defining conformance criteria and an accreditation program that will allow providers who meet the Standard's conformance criteria to become accredited and acknowledged on a public accreditation registry. Customers from industry and government can then use the registry to identify Trusted Technology Providers with increased confidence.

Adoption of these best practices and conformance criteria by component suppliers, by providers who include those components in their products, and by integrators who integrate components and products, will enable industry and government to manage commercial supply chain risk sustainably in a dynamic and globally-integrated environment. Thus, enabling Trusted Technology Providers to "build with integrity", and customers to "buy with confidence".

The Open Group has been acting as a vendor-neutral certification authority business for over 20 years - working with their forums to develop and operate certification programs, and working with other 3rd party consortia to develop and operate their certification programs as a vendor-neutral third party. The Open Group offers certification programs for: product certifications, skills and capabilities certifications, and best practice certifications. Some examples include: Unix®, TOGAF®, OpenCA (Certified Architect), OpenCITS (Certified IT Specialist), North American State and Provincial Lottery Association (NASPL), and one of our most recent for the NFC Forum. In some of these programs, the Open Group acts as the validator and for others we utilize third party laboratories for validations. For all of

them The Open Group operates and administers the certification program as the vendor-neutral 3rd party.

Standards Harmonization and Global Outreach is required

The Open Group leverages existing open standards to the greatest extent possible, including international standards such as International Organization for Standardization (ISO) and has recognized PAS (Publicly Available Specification) submitter status to ISO, which allows The Open Group to send specifications directly for country voting, to become ISO/IEC standards.

One important element of the Forum's work is our commitment to complement and interoperate with other relevant standards and industry practices. International standardization of the Standard is an important objective of their effort. Thus, last year the Forum's Standards Harmonization Work Stream conducted a review of the supply chain standards landscape. The Work Stream found that there were no other standards that covered the breadth of the Standard and no standard that addressed the depth of the Standard supply chain best practices. The Work Stream members did, however, identify standards and standards-type activities that had small areas of overlap. Given the desire to help assure that the standards would be harmonized and aligned as much as possible, the Forum is establishing liaisons and relationships with a range of organizations and working groups including:

- International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) Joint Technical Committee 1,

Information Technology Standards, Subcommittee 27, IT Security Techniques – where we have pending liaisons in two SC27 Working Groups:

  - WG3, Security Evaluation Criteria, which produces Common Criteria-related standards such as ISO/IEC 15408 and ISO/IEC 18045:
  - Working Group 4 (WG4), Security Controls and Services, which is producing ISO/IEC 27036 on Information Security for Supplier Relations

- InterNational Committee for Information Technology Standards (INCITS-CS1)
- National Security Agency (NSA)
- National Information Assurance Partnership (NIAP)
- National Institute of Standards and Technology (NIST)
- Communications-Electronics Security Group (CESG) - UK

The Forum is working globally with governments and international standards organizations to promote and harmonize this and future Standards directed at supply chain. The Forum wishes, where appropriate, to leverage existing evaluation and testing schemes while harmonizing with the security standards to which those schemes relate.

Conclusion:

Thank you for the opportunity to provide an overview of how The Open Group Trusted Technology Forum is addressing supply chain security. We offer up the expertise of the Forum to the Subcommittee and other Congressional committees as

they continue to examine supply chain issues. For additional information please feel free to contact me at d.lounsbury@opengroup.org. For a further look at The Open Group and to download the Snapshot please access the following links: The Open Group and The Open Trusted Technology Provider Standard Snapshot.

Appendix: Security Activities of The Open Group

Assuring the security of corporate data, information systems and critical infrastructure is a challenging task, requiring the joint efforts of customers, software and platform vendors, and governments. The Open Group hosts a variety of Forums, Work Groups and projects that address various aspects of the challenge of security.

The Security Forum focuses on Security Architecture and Information Security Management. The forum produces technical standards, guides, best practices, and other deliverables aimed at customer practitioners and vendors.

The Jericho Forum® provides thought leadership on enabling businesses to securely collaborate in a deperimeterized world. The Jericho Forum produces position papers, requirements, and guidance for customer organizations and security vendors.

The Real-time & Embedded Systems Forum provides core technology suppliers, integrators and customers with dependability through assuredness in the development of secure, reliable systems using open standards. The Forum delivers whitepapers, technical API standards, guides, and evaluation and certification programs.

The Open Group Trusted Technology Forum (OTTF) leads the development of a standard, which is a set of best practices for product engineering, secure development and supply-chain security. This standard is called the Open Trusted Technology Provider Standard (O-TTPS). The Forum is also working on marked accreditation and conformance programs for provider organizations that conform to the O-TTPS standard.

The Cloud Computing Work Group is doing work in the area of security for the Cloud and SOA. This group is working on reference architecture for Cloud security.

The Open Group's security-related projects and events:

- **Information Security Management:** The Open Group Information Security Management Maturity Model (O-ISM3) project strives to continually improve information security management. Our goal is to further develop O-ISM3, and to establish it as an open industry standard
- **Risk Management:** Risk management is fundamental to effectively securing information, IT assets, and critical business processes. The Open Group has produced important publications and projects in this business-critical area
- **Security Architecture:** As a hub where expertise in architecture development and security converge, The Open Group is uniquely qualified to lead the industry in establishing consistent, reliable standards for developing secure architectures
- **Security Standards:** With a long legacy in the development of important security standards, The Open Group continues to create security standards that promote the development of secure IT systems
- **Security Conferences:** The Open Group produces and hosts quarterly security conferences, held jointly with our Enterprise Architecture Practitioners

conferences. These events provide an interactive forum that fosters in-depth discussions with security leaders, and meaningful networking with peers.

Examples of published works include:

Security Certification Product Standards

X98SS Secure Communications Services

X98XS Baseline Security 98

Consortium Specifications

H072 Enterprise-Wide Security: Authentication & Single Sign-On

H073 Business Services Architecture

H074 Interoperability: Electronic Mail Systems

H075 Interoperability

H076 Enterprise-Wide Security

H077 Enterprise Directory Services Integration

Corrigenda

U039 X/Open Single Sign-On Service (XSSO) - Pluggable Authentication

U051 CDSA/CSSM Authentication: Human Recognition Service (HRS) API

Guides

G033 Manager's Guide to Data Privacy

G044 Introduction to Security Design Patterns

G052 Guide to Digital Rights Management

G061 Framework for Control over Electronic Chattel Paper

G081 Requirements for Risk Assessment Methodologies

G112 Open Enterprise Security Architecture (O-ESA)

G250 Manager's Guide to Information Security

G905 CDSA Explained, Second Edition

Preliminary Specifications

P441 Distributed Audit Service (XDAS)

P442 Generic Cryptographic Service API (GCS-API) Base

P702 X/Open Single Sign-On Service (XSSO) - Pluggable Authentication

Snapshots

S020 Security Interface Specifications: Auditing and Authentication

S307 GSS-API Security Attribute and Delegation Extensions

Technical Guides

C103 FAIR - ISO/IEC 27005 Cookbook

G031 Security Design Patterns

G206 Defining and Buying Secure Open Systems

G410 Distributed Security Framework (XDSF)

G801 Architecture for Public-Key Infrastructure (APKI)

Security Technical Standards

C013 CDSA/CSSM Authentication: Human Recognition Service (HRS) API V2

C081 Risk Taxonomy

C102 Open Information Security Management Maturity Model (O-ISM3)

C111 Open Automated Compliance Expert Markup Language (O-ACEML)

C441 Generic Security Service API (GSS-API) Base

C529 X/Open Baseline Security Services (XBSS)

C908 Authorization (AZN) API

C914 Common Security: CDSA and CSSM, Version 2 (with corrigenda)

C425 Systems Management: Backup Services API (XBSA)

Security Technical Studies

E605 Security in Federated Naming

E403 Security in Interworking Specifications

E503 Desktop Security

White Papers

W031 Intrusion Attack and Response Workshop (inc. Full Script)

W031A Intrusion Attack and Response Workshop

W075 Information Security Strategy, Version 1.0

W117 TOGAF® and SABSA Integration

W119 Security Principles for Cloud and SOA

W055 Guide to Security Architecture in TOGAF®ADM

W116 An Architectural View of Security for Cloud