Open Group Standard

Open Trusted Technology Provider™ Standard (O-TTPS) Version 1.1

Mitigating Maliciously Tainted and Counterfeit Products

Open Group Standard

Open Trusted Technology Provider™ Standard (O-TTPS), Version 1.1
(Technically identical to ISO/IEC 20243:2015)

ISBN: 1-937218-55-3

Document Number: C147

Published by The Open Group, July 2014.

Comments relating to the material contained in this document may be submitted to:

The Open Group, Apex Plaza, Forbury Road, Reading, Berkshire, RG1 1AX, United Kingdom

or by electronic mail to:

ogttf-admin@opengroup.org

Contents

List of Tables

List of Figures

Preface

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 – 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

Further information on The Open Group is available at www.opengroup.org.

The Open Group publishes a wide range of technical documentation, most of which is focused on development of Open Group Standards and Guides, but which also includes white papers, technical studies, certification and testing documentation, and business titles. Full details and a catalog are available at www.opengroup.org/bookstore.

Readers should note that updates – in the form of Corrigenda – may apply to any publication. This information is published at www.opengroup.org/corrigenda.

This Document

The Open Group Trusted Technology Forum (OTTF or Forum) is a global initiative that invites industry, government, and other interested participants to work together to evolve this Standard and other OTTF deliverables.

This Standard is the Open Trusted Technology Provider Standard (O-TTPS). The Standard has been developed by the OTTF and approved by The Open Group, through The Open Group Company Review process. There are two distinct elements that should be understood with respect to this Standard: the O-TTPF (Framework) and the O-TTPS (Standard).

The O-TTPF (Framework): The Framework is an evolving compendium of organizational guidelines and best practices relating to the integrity of Commercial Off-the-Shelf (COTS) Information and Communication Technology (ICT) products and the security of the supply chain throughout the entire product life cycle. An early version of the Framework was published as a White Paper in February 2011 (see Referenced Documents). The Framework serves as the basis for this Standard, future updates, and additional standards. The content of the Framework is the result of industry collaboration and research as to those commonly used commercially

reasonable practices that increase product integrity and supply chain security. The members of the OTTF will continue to collaborate with industry and governments and update the Framework as the threat landscape changes and industry practices evolve.

The O-TTPS (Standard): The O-TTPS is an open standard containing a set of guidelines that when properly adhered to have been shown to enhance the security of the global supply chain and the integrity of COTS ICT products. It provides a set of guidelines, requirements, and recommendations that help assure against maliciously tainted and counterfeit products throughout the COTS ICT product life cycle encompassing the following phases: design, sourcing, build, fulfillment, distribution, sustainment, and disposal.

Using the guidelines documented in the Framework as a basis, the OTTF is taking a phased approach and staging O-TTPS releases over time. This staging will consist of standards that focus on mitigating specific COTS ICT risks from emerging threats. As threats change or market needs evolve, the OTTF intends to update the O-TTPS (Standard) by releasing addenda to address specific threats or market needs.

The Standard is aimed at enhancing the integrity of COTS ICT products and helping customers to manage sourcing risk. The authors of this Standard recognize the value that it can bring to governments and commercial customers worldwide, particularly those who adopt procurement and sourcing strategies that reward those vendors who follow the O-TTPS best practice requirements and recommendations.

Note: Any reference to "providers" is intended to refer to COTS ICT providers. The use of the word "component" is intended to refer to either hardware or software components.

Intended Audience

This Standard is intended for organizations interested in helping the industry evolve to meet the threats in the delivery of trustworthy COTS ICT products. It is intended to provide enough context and information on business drivers to enable its audience to understand the value in adopting the guidelines, requirements, and recommendations specified within. It also allows providers, suppliers, and integrators to begin planning how to implement the Standard in their organizations. Additionally, acquirers and customers can begin recommending the adoption of the Standard to their providers and integrators.

Trademarks

Acknowledgements

The Open Group acknowledges the contribution of the following people and organizations in the development of this Standard (presented in alphabetical order).

In particular we would like to provide a special thank you and acknowledgement to the Chair and Vice Chair of the OTTF: Andras Szakal, IBM (Chair) and Edna Conway, Cisco Systems (Vice Chair).

The contributing members of The Open Group Trusted Technology Forum (OTTF):

Contributors	**Organization**
Jon Amis	Dell, Inc.
Paul Aschwald	Hewlett-Packard Company
Nadya Bartol	(formerly of) Booz Allen Hamilton
James Bean	Juniper Networks
Kristen Baldwin	US DoD AT&L
Terry Blevins	MITRE
Joshua Brickman	CA Technologies
Stan Brown	CA Technologies
Ben Calloni	Lockheed Martin
Suresh Cheruserri	(formerly of) Tata Consultancy Services
YouHong (Robert) Chu	Kingdee Software
Erv Comer	Motorola Solutions
Erin Connor	Electronic Warfare Associates (EWA) – Canada Ltd.
Tammy Compton	(formerly of) SAIC
Edna Conway	Cisco Systems Inc. OTTF Vice-Chair
Don Davidson	DOD-CIO
Mary Ann Davidson	Oracle Corporation
Charles Dekle	(formerly of) US DoD AT&L
Terrie Diaz	Cisco Systems Inc.
Robert Dix	Juniper Networks
Holly Dunlap	Raytheon Company
Bob Ellison	SEI
Marcus Fedeli	(formerly of) NASA

Contributors	Organization
Luke Forsyth	CA Technologies
Susan Fultz	Hewlett-Packard Company
Steve Goldberg	(formerly of) Motorola Solutions
Tim Hahn	IBM Corporation
Wes Higaki	Apex Assurance Group
Ken Hong Fong	(formerly of) US DoD AT&L
Helmut Kurth	atsec information security
Mike Lai	Microsoft Corporation
David Ling	Hewlett-Packard Company
Steve Lipner	Microsoft Corporation O-TTPF Work Stream Co-Chair
Dr. David McQueeney	IBM Corporation
Jim Mann	Hewlett-Packard Company
Al Marshall	NASA
Michele Moss	Booz-Allen Hamilton
Shawn Mullen	IBM Corporation
Fiona Pattinson	atsec information security
Brendan Peter	CA Technologies
Glenn Pittaway	Microsoft Corporation
Andy Purdy	Huawei Technologies
Dan Reddy	EMC Corporation
Karen Richter	IDA
Jim Robinson	Hewlett-Packard Company
Hart Rossman	(formerly of) SAIC
Mark Schiller	(formerly of) Hewlett-Packard Company
Thomas Stickels	MITRE
Andras R. Szakal	IBM Corporation OTTF Chair and O-TTPF Work Stream Co-Chair
Steve Whitlock	The Boeing Company
Jim Whitmore	IBM Corporation
Robert Williamson	SAIC
Eric Winterton	Booz Allen Hamilton
Joanne Woytek	NASA
Chee Wai Foong	Cisco Systems Inc.

The individuals providing early contributions to this work:

Contributor	Name
Randy Barr	Qualys
Rance DeLong	LynuxWorks
Chris Fagan	(formerly of) Microsoft Corporation
Rob Hoffman	High Assurance Systems, Inc.
Dave McDermitt	(formerly of) SAIC
Terry Morgan	(formerly of) Cisco Systems Inc.
Paul Nicholas	Microsoft Corporation
Kerri Patterson	(formerly of) Cisco Systems Inc.
Steve Venema	The Boeing Company
Larry Wagoner	NSA

The Open Group staff:

Name	Role
James Andrews	The Open Group Conformance Quality Manager
Joe Bergmann	Open Group Government Relations, Director, RT&ES
James de Raeve	VP Certification
Cathy Fox	Technical Editor
Jim Hietala	VP Security
Andrew Josey	Director, Standards
Sally Long	Director, The Open Group Trusted Technology Forum (OTTF)
Dave Lounsbury	Chief Technical Officer

Referenced Documents

The following documents are referenced in this Standard:

- 2007 Defense Science Board Task Force on Mission Impact of Foreign Influence on DoD Software, September 2007; findings and recommendations located at: www.acq.osd.mil/dsb/reports/ADA486949.pdf.
- Electronic Industry Citizenship Coalition (EICC) Code of Conduct; refer to: www.eicc.info.
- ISO/IEC 15408: Information Technology – Security Techniques – Evaluation Criteria for IT Security (Common Criteria).
- ISO/IEC 27000:2009: Information Technology – Security Techniques – Information Security Management Systems – Overview and Vocabulary.
- ISO/IEC Directives, Part 2: Rules for the Structure and Drafting of International Standards.
- NIST 800-12: An Introduction to Computer Security: The NIST Handbook.
- White Paper: Open Trusted Technology Provider Framework (O-TTPF), W113, published by The Open Group, February 2011; refer to: www.opengroup.org/bookstore/catalog/w113.htm.

1 Introduction

This chapter introduces this Standard – the Open Trusted Technology Provider Standard (O-TTPS) – and the normative terminology that should be understood in relation to specific requirements and recommendations found in Chapter 4 of this document.

1.1 Objectives

The Open Trusted Technology Provider Standard (O-TTPS) is a set of guidelines, requirements, and recommendations that, when practically applied, create a business benefit in terms of reduced risk of acquiring maliciously tainted or counterfeit products for the technology acquirer. Documenting 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 this Standard, can provide significant advantage in establishing a basis to reduce risk. A commitment by technology providers, large and small, suppliers of hardware and software components, and integrators to adopt this Standard is a commitment to using specific methodologies to assure the integrity of their hardware or software Commercial Off-the-Shelf (COTS) Information and Communication Technology (ICT) products. This Standard is detailed and prescriptive enough 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.

1.2 Overview

This Standard (O-TTPS) is a set of guidelines, requirements, and recommendations that address specific threats to the integrity of hardware and software COTS ICT products throughout the product life cycle. This initial release of the Standard addresses threats related to maliciously tainted and counterfeit products.

The provider's product life cycle includes the work it does designing and developing products, as well as the supply chain aspects of that life cycle, collectively extending through the following phases: design, sourcing, build, fulfillment, distribution, sustainment, and disposal. While this Standard cannot fully address threats that originate wholly outside any span of control of the provider – for example, a counterfeiter producing a fake printed circuit board assembly that has no original linkage to the Original Equipment Manufacturer (OEM) – the practices detailed in the Standard will provide some level of mitigation. An example of such a practice would be the use of security labeling techniques in legitimate products.

The two major threats that acquirers face today in their COTS ICT procurements, as addressed in this Standard, are defined as:

1. Maliciously tainted product – the product is produced by the provider and is acquired through a provider's authorized channel, but has been tampered with maliciously.

2. Counterfeit product – the product is produced other than by, or for, the provider, or is supplied to the provider by other than a provider's authorized channel and is presented as being legitimate even though it is not.

Note: All instances, within this standard, of the use of the words: taint, tainted, tainting, refer to maliciously taint, maliciously tainted, and maliciously tainting, respectively.

Trusted Technology Providers manage their product life cycle, including their extended supply chains, through the application of defined, monitored, and validated best practices. The product's integrity is strengthened when providers and suppliers follow the requirements and recommendations specified in this Standard. The industry consensus reflected here and in the Open Trusted Technology Provider Framework (O-TTPF) draws from the following areas that are integral to product integrity: product development/engineering, secure development/engineering, and supply chain security. Additionally, product integrity and supply chain security are enhanced by following practices among suppliers, trading partners, providers, and, when appropriate, acquiring customers to preserve the product's intended configuration.

This Standard is focused on the security of the supply chain *versus* the business management aspects of the supply chain. This Standard takes a comprehensive view about what providers should do in order to be considered a Trusted Technology Provider that "builds with integrity". This includes practices that providers incorporate in their own internal product life cycle processes, that portion of product development that is "in-house" and over which they have more direct operational control. Additionally, it includes the provider's supply chain security practices that need to be followed when incorporating third-party hardware or software components, or when depending on external manufacturing and delivery or supportive services.

The Standard makes a distinction between provider and supplier. Suppliers are those upstream vendors who supply components or solutions (software or hardware) to providers or integrators. Providers are those vendors who supply COTS ICT products directly to the downstream integrator or acquirer.

Ideally, the guidelines, requirements, and recommendations included in this Standard will be widely adopted by providers and their suppliers regardless of size and will provide benefits throughout the industry.

For this version of the Standard, the following elements are considered out of scope:

- This Standard does not focus on guidelines, requirements, and recommendations for the acquirer. The Forum is considering addressing this area in subsequent versions of the Standard. In the meantime, an acquirer does have a role to play in assuring that the products and components they procure are built with integrity. One of the ways that the acquirer can do that is to require their providers, suppliers, and integrators to be Trusted Technology Providers. Another way is to not knowingly support the "grey market", realizing that if an acquirer elects to receive hardware or software support from grey market suppliers, it is at their own risk and generally outside of the influence of the legitimate provider.
- This Standard is not meant to be comprehensive as to all practices that a provider should follow when building software or hardware. For a more comprehensive set of foundational

best practices that a provider could implement to produce good quality products, readers can refer to the O-TTPF White Paper.

- This version of the Standard does not apply to the operation or hosting infrastructure of on-line services, but can apply to COTS ICT products in as far as they are utilized by those services.

This Standard complements existing standards covering product security functionality and product information assurance, such as ISO/IEC 15408 (Common Criteria).

1.3 Conformance

The OTTF intends to develop conformance criteria and create an Accreditation Policy and Program for the Open Trusted Technology Provider Standard (O-TTPS) as a useful tool for all constituents with an interest in supply chain security. Without the associated conformance criteria and an Accreditation Program, there is no assurance that an organization has implemented practices according to the O-TTPS.

Accreditation will provide formal recognition of conformance to the O-TTPS, which allows:

- Providers and practitioners to make and substantiate clear claims of conformance to the Standard
- Acquirers to specify and successfully procure from providers who conform to the Standard

Conformance assessment is the act of determining the conformance of an implementation to a specification, or the adherence of a business operation to a best practice or process definition. There are many techniques for assessing such conformance, including the use of a standardized test method, quality assessment by industry experts or third-party test laboratories, and vendors' claims of conformance made within a defined legal framework.

The O-TTPS accreditation process, conformance criteria, conformance assessment, policies, parties, and their roles will be defined and approved after the publication of Version 1.0 of this Standard.

1.4 Terminology

This section provides a set of terms and their definitions, which should be used when describing and interpreting the Standard requirements and recommendations specified in Chapter 4 of this Standard. These terms are aligned with ISO/IEC Directives, Part 2 (Annex H).

Shall	Indicates an absolute, mandatory requirement of the Standard that has to be implemented in order to conform to the Standard and from which no deviation is permitted. Do not use "must" as an alternative for "shall". (This will avoid any confusion between the requirements of a document and external statutory obligations.)

Shall not	Indicates an absolute preclusion of the Standard, and if implemented would represent a non-conformity with the Standard. Do not use “may not” instead of “shall not” to express a prohibition.
Should	Indicates a recommendation among several possibilities that is particularly suitable, without mentioning or excluding others, or that a certain course of action is preferred but not necessarily required.
Should not	Indicates a practice explicitly recommended not to be implemented, or that a certain possibility or course of action is deprecated but not prohibited. To conform to the Standard, an acceptable justification must be presented if the requirement is implemented.
May	Indicates an optional requirement to be implemented at the discretion of the practitioner. Do not use “can” instead of “may” in this context.
Can	Used for statements of possibility and capability, whether material, physical, or causal.

1.5 Future Directions

The OTTF intends to address possible additional threats and risks with best practice requirements and recommendations in future Standard releases. The OTTF also intends to provide conformance criteria and an O-TTPS Accreditation Program.

2 Business Context and Overview

This chapter describes the typical business environment, the business rationale, the context of Commercial Off-the-Shelf (COTS) Information and Communication Technology (ICT), and an overview of the Open Trusted Technology Provider Framework (O-TTPF) and this Open Trusted Technology Provider Standard (O-TTPS).

2.1 Business Environment Summary

Globalization is inherent in the business environment. The rapid pace of globalization has brought both benefits and risks to customers of COTS ICT products. Globalization is an essential factor in the ability to build, deliver, and support feature-rich COTS ICT hardware and software, and the economies of scale resulting from globalization are a significant benefit. In fact, in today's market COTS ICT products could not exist without global development – the global production environment is essential to the technology industry.

As cyber attacks increase in sophistication, stealth, and severity, global governments and larger enterprises have also begun to take a more comprehensive approach to risk management as it applies to product integrity and supply chain security. In addition to enhancing information security by improving security practices across the enterprise, governments and enterprises have begun inquiring about the practices COTS ICT vendors use to protect the integrity of their products and services as they are developed and moved through the global supply chain. First, one needs to understand the extent of the global supply chain by looking at an operational scenario.

2.1.1 Operational Scenario

Figure 1 provides one example of how the various constituents in COTS ICT product supply chains ideally would interact. These constituents may not always have a role to play in every scenario. They are all included to provide a more complete picture.

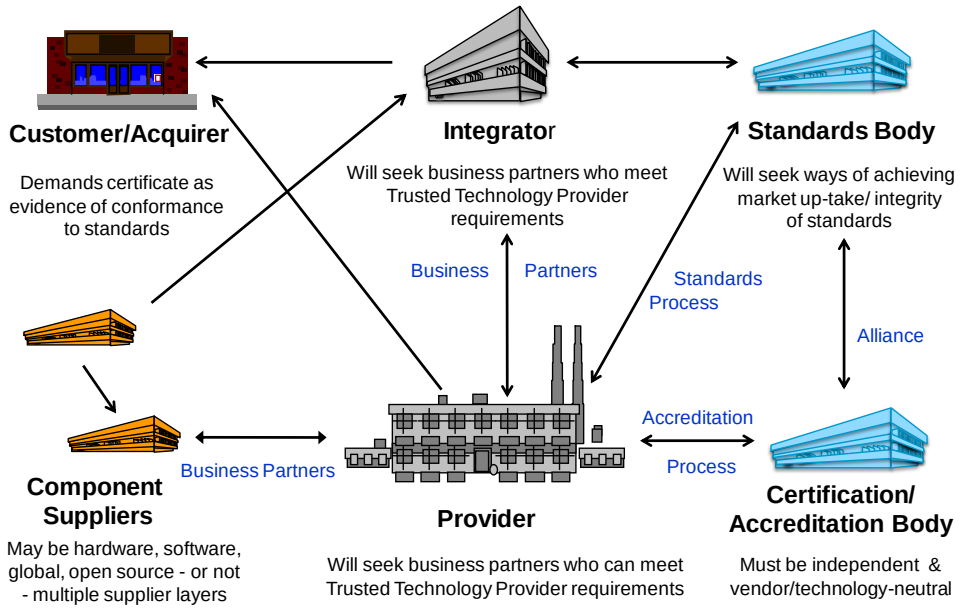

Figure 1: Constituents

Table 1 describes the roles of these constituents in this Standard.

Table 1: O-TTPS Constituents and their Roles

Constituent	Role Played
Customer	Synonymous with acquirer.
Acquirer	Acquires or procures a product or service from a supplier, provider, or integrator. Procures and integrates components, products, and services to create solutions that meet the customer's requirements. Downstream customer or integrator.
System Integrator	Provides services and solutions to customers. Typically used on large projects that deal with multiple providers. Engages in competitive tendering processes with acquirers. Has alliances with providers and acquirers. Deals with the incorporation of technologies that could be component technologies as sub-assemblies or component technologies incorporated into assemblies. These assemblies could be hardware assemblies, software assemblies, or combinations of hardware and software.
Vendor	Synonymous with provider.

Constituent	Role Played
Provider	Builds products, either entirely in-house, or including software and/or hardware components from suppliers. Has alliances with: acquirers, integrators, suppliers (for software or hardware components), and business partners, including distribution channel partners. May also utilize Open Source software components in development of their products. May engage in the standards process with standards bodies. Engages in the certification/accreditation process with certification/accreditation bodies. Requests that their suppliers follow the O-TTPS and have been accredited as Trusted Technology Providers. Builds products that may be the subject of certification. Develops products and manages the supply chain to provide acquirers and integrators with trustworthy products.
Supplier	Supplies components typically as a business partner to providers. May be required to prove that their products meet certain criteria through certification or through vendor test and documentation procedures. Has business partnerships with providers. May also be a provider in its own right.
Standards Body	Develops technical specifications that establish some of the criteria for certification. Engages in the standards process with providers, customers, and integrators. Has alliances with certification/accreditation bodies.
Certification/ Accreditation Body	Provides certification and/or testing services, especially those involved with conformance certification and/or testing. Has alliances with standards bodies. Engages in the certification/accreditation process with vendors.

2.2 Business Rationale

The following sections provide the business rationale for the Standard by presenting the business drivers and benefits. Section 2.3 provides more context on what this Standard can and cannot reasonably cover.

2.2.1 Business Drivers

Both acquirers and providers understand the need for globalization and wish to gain visibility into the risks inherent in global sourcing for product development and manufacturing. Governments and commercial consumers have expressed specific interest in understanding the risks and learning how providers manage those risks by asking the providers the following questions:

- What potential security risks may be inherited from supply chains, both for software and hardware, and how does the Original Equipment Manufacturer (OEM) assess and manage these risks?
- What supply chain security practices can mitigate potential risks of significant supply chain attacks?
- What are the risks to confidentiality, integrity, and availability of a customer's environment or critical infrastructure as a result of procurement by customers of counterfeit components and products?
- What software or technology development or engineering practices can help reduce product integrity risks?
- How is product integrity and risk managed through the adoption of industry best practices and assurance programs?

Because COTS ICT products are used extensively in both private industry and government acquisition, an alignment of interests exists between enterprise customers and government customers. There is a shared business value in understanding the factors that contribute to the integrity of COTS ICT products and supply chain security, identifying those practices that can improve product integrity and supply chain security, accrediting providers who follow those best practices, and knowing how to identify trustworthy products that were built by Trusted Technology Providers.

2.2.2 Objectives and Benefits

The technology supply chain continues to become more globalized, segmented, and specialized. All commercial and government acquirers, integrators, software developers, hardware providers, and manufacturers are members of the global technology supply chain. Consequently, every member of this global community has a responsibility to ensure the security of the end-to-end technology supply chain. The Open Group Trusted Technology Forum (OTTF) is intended to facilitate the evolution of the O-TTPF (Framework) and O-TTPF-related Standards to allow compliant providers to address the ever-changing supply chain landscape and new threats as they emerge.

The OTTF also intends to provide an accreditation program that will allow providers who meet the O-TTPS requirements and recommendations to become accredited and acknowledged on a public accreditation registry, so that customers from industry and government can buy from those Trusted Technology Providers with increased confidence.

The Forum's work is intended to benefit:

- **Providers**: Providers who adopt these practices will be better able to identify and mitigate security risks throughout the development, sourcing, and maintenance of COTS ICT products. They will be able to take advantage of a market differentiator associated with Trusted Technology Provider status, and to more readily identify Trusted Technology Providers for their own supplier and business partner relationships.
- **Suppliers**: Suppliers who follow these best practice requirements and recommendations can also achieve Trusted Technology Provider status and will be able to take advantage of

a market differentiator associated with having that status, which could result in better and more frequent business partnerships among Trusted Technology Providers and integrators.

- **Integrators**: Integrators will be able to buy products and components (hardware and software) from Trusted Technology Providers and suppliers enabling that part of their integration work that is based on out-sourcing and partnerships, to be more secure and trustworthy. In addition, integrators who follow the O-TTPS and are Trusted Technology Providers will realize the same benefits as the providers (above).
- **Acquirers**: Acquirers will be able to consider a provider's adherence to the O-TTPS as one element of their own comprehensive commercial technology procurement and risk management strategy.
- **Marketplace at Large**: Over time, widespread use of and/or reference to the OTTF's work products will help realize security enhancements throughout the global information infrastructure in a manner that promotes trust, accountability, and global innovation.

By working together, the members of the OTTF have brought to the table their own best practices and have created a composite set of best practice requirements and recommendations to be codified in this and future Standards. The OTTF work is notable in representing consensus for commercially reasonable best practices from industry in addressing the threats in focus. Once the Standards have been approved and published they will be available for large and small organizations throughout the world, to reference and incorporate into their practices with the intent of raising the bar for all providers and component suppliers. This, in and of itself, would be a major benefit for global providers and customers, including governments.

2.3 Recognizing the COTS ICT Context

It is important in defining this Standard of best practice requirements and recommendations, to outline the COTS ICT context and limitations. Identifying self-imposed and practical limitations enables businesses to focus upon making improvements in those critical areas that will help to deliver the practical improvements at the heart of this Standard. Clearly stating such limitations is essential to avoiding effort not focused on tangible improvements; for example:

- Addressing unsolvable problems
- Allowing scope to creep beyond succinctly constructed problem statements

Equally important to optimizing this Standard is limiting focus to those supply chain risks that are specifically associated with a targeted supply chain attack. There is a clear difference between the variety of supply chain business risks (e.g., a supplier going out of business or selling a bad product) and those risks associated with a targeted supply chain attack (e.g., someone maliciously corrupting a component within a product being sold). Two of the principal targeted attack areas relate to tainted and counterfeit products. Suppliers and customers should rightly be concerned about these areas and they are discussed in Chapter 3 of this Standard. A focus on best practices in these risk areas is likely to lead to the critical improvements that both buyers and sellers want, and an improved global market encompassing trustworthy suppliers and trustworthy products.

Many other business risks are of concern but do not represent targeted *attacks* on the supply chain and are thus not a focus area of these best practices. One such area is the risk pertaining to a poor quality product. In the case of software and hardware, product defects include unintended mistakes in coding or unintended mistakes in design. The cost of having to apply multiple patches to address software defects is in some cases a "hidden cost" and may affect both a system's overall cost and effectiveness. Providers, too, have a vested interest in reducing unintended defects since they may damage their brand and add business costs via creating and testing patches. However, the nature of software and hardware development is as follows:

- It is impossible to verify that a component or product is free from all defects.
- Some defects are "security vulnerabilities"; i.e., defects may be exploited by knowledgeable users to bypass security mechanisms.
- Once security vulnerabilities are exploited there may be a compromise in the confidentiality, integrity, or availability of systems containing the component or product.

This is true for any software or hardware component, including government developed and COTS ICT.

However important the area of "vulnerabilities" is to both buyers and sellers, it is a risk of buying *any* product. While vulnerabilities can never be completely eradicated, this Standard does provide best practice requirements that will help to limit them, including a set of best practice requirements specifically related to vulnerability analysis and response.

Another property inherent in the use of COTS software and hardware requires that consumers (acquirers) understand that COTS products are intended to meet the needs of a specific commercial market segment. Whether a software or hardware product is "fit-for-purpose", including "fit for the security threats it will face", is a business and system design decision that must be understood by the customer, since COTS by definition is *not* "special-purpose, custom design". Thus, "determination of fitness-for-purpose" is not part of the scope of the best practices in this Standard.

Lastly, even though "tainting" is rightly a focus area of this Standard, there are limitations of best practices in ameliorating certain tainting risks. Chief among these is the problem of a malicious yet fully authorized insider deliberately corrupting or tainting product; that is, putting in unintended functionality (e.g., a backdoor allowing bad actor access) or corrupting functionality (e.g., rendering access controls by-passable under some conditions). It is, in short, impossible to completely prevent a fully authorized insider from changing code in a way that is undetectable, even if you know where to look for the corrupt code.[1] The practices described here may be applied to mitigate risks introduced by both malicious insiders and outsiders.

Recognizing these COTS ICT realities and given the continual improvement in vulnerability analysis tools and techniques, this Standard does identify best practice requirements and recommendations in those areas of risk. If followed in conjunction with the other best practice requirements identified in the Standard, they will help to reduce the possibility of malicious code being introduced as the product progresses throughout its life cycle and measurably further the

[1] For support of this premise, see the 2007 Defense Science Board Task Force on Mission Impact of Foreign Influence on DoD Software. It is not currently a solvable problem, or even a problem for which there are acceptable mitigation techniques.

goal of an improved global market encompassing trustworthy suppliers and trustworthy products.

2.4 Overview

This section provides overviews of the Framework and the O-TTPS (Standard), and adds findings from the Standards Harmonization Work Stream of the OTTF.

2.4.1 O-TTPF Framework Overview

This section addresses the Framework for reference purposes only and to provide context. The Standard for mitigating tainted and counterfeit products is addressed in subsequent sections.

The Framework organizes best practices into the following four categories:

- Product Development/Engineering Method
- Secure Development/Engineering Method
- Supply Chain Security Method
- Product Evaluation Method

The best practices within these methods are those considered most effective in protecting customers from assuming unacceptable levels of product integrity and supply chain security risks. The methods identify fundamental areas within the development and manufacturing process where risk management and assurance have the greatest impact on the quality and integrity of a COTS ICT product. These practices and methods are anticipated to evolve as new common approaches and techniques are identified and adopted by Trusted Technology Providers.

The first three methods identified above are in scope for this Standard. The concept of a Product Evaluation Method as referenced in the Framework is focused specifically on product security. This version of the Standard, however, expressly excludes from its scope best practice requirements for the evaluations of product security functionality and information assurance of individual products.

While the best practice requirements and recommendations found in this Standard have been derived from and informed by the broad Framework method categories, only those requirements and recommendations that pertain directly to the two specific risks identified in Chapter 3 – namely, tainted and counterfeit products – are set forth in this Standard.

A publically available early version of the Framework can be found in the White Paper (see Referenced Documents).

2.4.2 Standard Overview

In releasing standards based on the Framework to the global community, the OTTF decided to scope this version of the Standard to best practice requirements and recommendations for reducing the threats, and mitigating the risks associated with, tainted and counterfeit products.

The organization of the best practice requirements and recommendations in this Standard are presented in two categories of product life cycle activities:

1. Technology Development
2. Supply Chain Security

2.4.3 Relationship with Other Standards

The Forum's Standards Harmonization Work Stream conducted a standards landscaping exercise in 2011. At the time the landscaping exercise was completed, the findings of the Work Stream were that there were no other standards that covered the breadth of the O-TTPS and no standard that addressed the depth of the O-TTPS supply chain best practices. The Work Stream members did, however, identify standards and standards-type activities for harmonization. Given the desire to help assure that the standards would be harmonized and aligned as much as possible, the OTTF established liaisons and is working with a range of organizations and working groups including the International Organization for Standardization/International Electrotechnical Commission (ISO/IEC).

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

3 O-TTPS – Tainted and Counterfeit Risks

This chapter highlights certain risks associated with tainted and counterfeit Commercial Off-the-Shelf (COTS) Information and Communication Technology (ICT) products. The following chapter, Chapter 4, specifies the requirements and recommendations of this Open Trusted Technology Provider Standard (O-TTPS) that, when implemented by Trusted Technology Providers, are designed to reduce those risks.

As defined in Chapter 1, a tainted product is a product that is produced by the provider and is acquired through a provider's authorized channel but has been tampered with maliciously. A counterfeit product is produced other than by or for the provider, or is supplied by other than a provider's authorized channel, and is represented as legitimate. For example, a provider could source from a supplier that supplies a product that purports to be from Vendor X, but is, instead, a "fake".

Counterfeiting poses significant risk to an organization because the integrity of a "fake" product cannot be validated. In addition, counterfeit products are unsupported by the original provider and can often result in significant financial and productivity losses. This damages the customer, whose purchased product may fail at a critical juncture, as well as the supplier, whose revenue stream and brand may be damaged due to a fake, inferior product. Even in cases where the "fake" is a bit-for-bit copy of the original, a customer may be damaged by the inability to get support services for a counterfeit product, and the supplier is damaged by loss of the revenue stream that should rightly accrue from their intellectual property.

Tainting is important for similar reasons: a corrupted product may not perform as intended. In fact, the tainting may well be for the precise reason of causing the product not to perform as intended, thus enabling a specific attack on an entity using the tainted product. Failure, degraded performance, rogue functionality, and weakened security mechanisms are all possible outcomes of tainted products.

The concepts of tainted and counterfeit products can be confusing, so some examples of threats relating to each concept are presented here to provide some useful clarification. An example of a threat relating to a tainted product is "malware", which can be thought of as the introduction of unauthorized functionality into an otherwise genuine product, with the purpose of producing an outcome undesirable for the provider and/or the acquirer.

An example of a threat relating to a counterfeit product is the use of scrap or sub-standard parts; specifically, the introduction of parts into the supply chain that have been discarded at some earlier stage of the supply chain, either through failing to meet a quality bar, or having reached their end-of-life.

In addition to understanding the concepts of tainted and counterfeit products and their associated risks, supply chain discussions require understanding of where in the chain those risks may be relevant. From a provider's perspective, technology development and supply chain activities can be said to have "upstream" and "downstream" elements. "Upstream" of the provider are

suppliers of components (software or hardware); for example, driver developers or chip manufacturers. "Downstream" are the integrators and distribution channels, from which acquirers source their products. Understanding the relevance of specific risks in this continuum informs the measures that can be taken by providers in mitigating risk; for example, upstream risks can be mitigated somewhat by contractual language, acceptance procedures, etc. Table 2 illustrates this dimension for both tainted and counterfeit products in relation to some of the more serious risks, specifically:

- **Malware**: Functionality that intentionally undermines or defeats the confidentiality, integrity, or availability of a system or data (e.g., viruses, worms, or other malicious code, whether detected by signature-based anti-malware programs or not).
- **Unauthorized "Parts"**: The introduction into a product or component of a potentially dangerous component that is unauthorized (e.g., a microprocessor device driver masquerading as being from a provider's authorized channel).
- **Unauthorized Configuration**: The introduction of potentially dangerous changes to control settings, attack surface, etc.
- **Scrap/Sub-standard Parts**: The introduction of parts into the supply chain that have been discarded at some earlier stage of the supply chain, either through failing to meet a quality bar, or having reached their end-of-life.
- **Unauthorized Production**: Products that are not authorized for manufacture or sale (e.g., the unauthorized production and sale of parts or products, by a manufacturing partner authorized to produce those parts or products on behalf of a provider).

In Table 2, the designation "Relevant" indicates that a specific risk can be thought of arising at a particular stage in the continuum.

Table 2: Threat Mapping

	Tainted			**Counterfeit**		
	Upstream	Provider	Downstream	Upstream	Provider	Downstream
Malware	Relevant	Relevant	Relevant			
Unauthorized "Parts"	Relevant	Relevant	Relevant	Relevant		
Unauthorized Configuration			Relevant			
Scrap/Sub-standard Parts				Relevant		
Unauthorized Production				Relevant		Relevant

4 O-TTPS – Requirements for Addressing the Risks of Tainted and Counterfeit Products

This chapter defines the requirements and recommendations relating to tainted and counterfeit product risks for this version of the Open Trusted Technology Provider Standard (O-TTPS).

Note: It is important to understand that all of the requirements and recommendations listed in the tables in this chapter are specified using prescriptive terms (e.g., shall, should, may); for definitions of these terms, please refer to the definitions in Section 1.3 (Terminology). For reasons of consistency, these terms are equivalent to the corresponding ISO definitions.

This Standard is described in terms of the provider's product life cycle. The collection of provider best practices contained in the O-TTPS are those that the OTTF considers best capable of influencing and governing the integrity of a Commercial Off-the-Shelf (COTS) Information and Communication Technology (ICT) product from its inception to proper disposal at end-of-life. These provider practices are divided into two basic categories of product life cycle activities as described in Section 2.4.2: Technology Development and Supply Chain Security:

- The provider's Technology Development activities for a COTS ICT product are mostly under the provider's in-house supervision in how they are executed. The methodology areas that are most relevant to assuring against tainted and counterfeit products are: Product Development/Engineering methods and Secure Development/Engineering methods.
- The provider's Supply Chain Security activities focus on best practices where the provider must interact with third parties who produce their agreed contribution with respect to the product's life cycle. Here, the provider's best practices often control the point of intersection with the outside supplier through control points that may include inspection, verification, and contracts.

While these categories are useful as an organizing construct, they are not absolute distinctions; for example, one product may be handled by the provider's own organization exclusively, whilst another product's life cycle could involve many aspects being handled in conjunction with a variety of third parties as governed by the provider. These two major categories of the product life cycle are depicted in Figure 2:

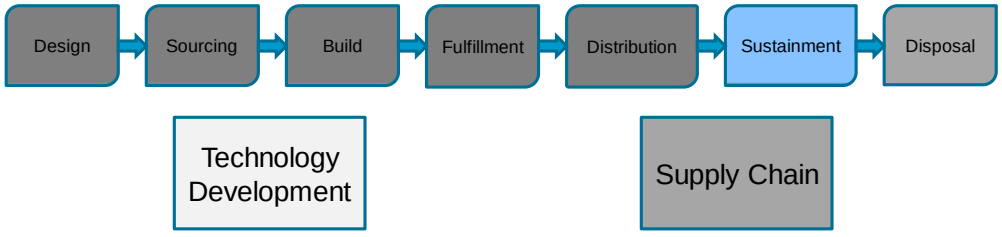

Figure 2: Product Life Cycle – Categories and Activities

For structural purposes, in Sections 4.1 and 4.2, the requirements and recommendations are delineated in separate sections according to which of the two major categories they fit into – Technology Development and Supply Chain Security. However, from an operational perspective, there is some overlap between best practices that might be followed in-house during Technology Development, and those that might be invoked between a supplier and a provider at a particular interface in the Supply Chain. The shading in the diagram above depicts an example of this overlap of boundaries.

The following sections include the prescriptive requirements and recommendations for this Standard. The requirements are focused on the two identified threats. Some are highly correlated to the specific threats; others are more foundational but considered essential.

4.1 Technology Development

For purposes of addressing tainted and counterfeit products, the Technology Development category of the product life cycle reflects the following methods, which are referred to in Section 4.1.1 and Section 4.1.2:

1. Product Development/Engineering Method: Trusted Technology Providers use a well-defined, documented, and repeatable product development or engineering method and/or process. The effectiveness of the method is managed through metrics and management oversight.

2. Secure Development/Engineering Method: Trusted Technology Providers employ a secure engineering method when designing and developing their products. Software providers and suppliers often employ methods or processes with the objective of identifying, detecting, fixing, and mitigating defects and vulnerabilities that could be exploited, as well as verifying the security and resiliency of the finished products. Hardware providers and suppliers also include ways to mitigate use of unverified and inauthentic software and to protect against counterfeit hardware or software.

4.1.1 PD: Product Development/Engineering Method

The following sections contain the best practice requirements and recommendations primarily associated with the Technology Development category of activities relating to the product development/engineering method.

4.1.1.1 PD_DES: Software/Firmware/Hardware Design Process

Attribute Definition

A formal process exists that defines and documents how requirements are translated into a product design.

Requirements

PD_DES.01	A process shall exist that assures the requirements are addressed in the design.
PD_DES.02	Product requirements shall be documented.

PD_DES.03	Product requirements should be tracked as part of the design process.

4.1.1.2 PD_CFM: Configuration Management

Attribute Definition

A formal process and supporting systems exist which assure the proper management, control, and tracking of change to product development and manufacturing assets and artifacts.

Requirements

PD_CFM.01	A documented formal process shall exist which defines the configuration management process and practices.
PD_CFM.02	Baselines of identified assets and artifacts under configuration management shall be established.
PD_CFM.03	Changes to identified assets and artifacts under configuration management shall be tracked and controlled.
PD_CFM.04	Configuration management should be applied to build management and development environments used in the development/engineering of the product.
PD_CFM.05	Access to identified assets and artifacts and supporting systems shall be protected and secured.
PD_CFM.06	A formal process shall exist that establishes acceptance criteria for work products accepted into the product baseline.

4.1.1.3 PD_MPP: Well-defined Development/Engineering Method Process and Practices

Attribute Definition

Development/engineering processes and practices are documented, and managed and followed across the life cycle.

Requirements

PD_MPP.01	The development/engineering process as documented should be inclusive of development partners as defined by the governance process.
PD_MPP.02	The development/engineering process shall be able to track, as appropriate, components that are proven to be targets of tainting or counterfeiting as they progress through the life cycle.

4.1.1.4 PD_QAT: Quality and Test Management

Attribute Definition

Quality and test management is practiced as part of the product development/engineering life cycle.

Requirements

PD_QAT.01	There shall be a quality and test product plan that includes quality metrics and acceptance criteria.
PD_QAT.02	Testing and quality assurance activities shall be conducted according to the plan.
PD_QAT.03	Products or components shall meet appropriate quality criteria throughout the life cycle.

4.1.1.5 PD_PSM: Product Sustainment Management

Attribute Definition

Product support, release maintenance, and defect management are product sustainment services offered to acquirers while the product is generally available.

Requirements

PD_PSM.01	A release maintenance process shall be implemented.
PD_PSM.02	Release maintenance shall include a process for notification to acquirers of product updates.
PD_PSM.03	Release maintenance shall include a product update process, which uses security mechanisms.
PD_PSM.04	A defect management process shall be implemented.
PD_PSM.05	The defect management process shall include: a documented feedback and problem reporting process.

4.1.2 SE: Secure Development/Engineering Method

The following sections contain the best practice requirements and recommendations primarily associated with the Technology Development category of activities relating to the secure development/engineering method.

4.1.2.1 SE_TAM: Threat Analysis and Mitigation

Attribute Definition

Threat analysis and mitigation identify a set of potential attacks on a particular product or system and describe how those attacks might be perpetrated and the best methods of preventing or mitigating potential attacks.

Requirements

SE_TAM.01	Product architecture and design shall be assessed against potential attacks to gain an understanding of the threat landscape.

SE_TAM.02	Threat mitigation strategies for tainted and counterfeit products shall be implemented as part of product development.
SE_TAM.03	Threat analysis shall be used as input to the creation of test plans and cases.

4.1.2.2 SE_RTP: Run-time Protection Techniques

Attribute Definition

Run-time protection techniques are considered part of a secure development/engineering method. This includes techniques to mitigate the exploitation of vulnerabilities. For example, run-time protection techniques help defend executable code against buffer overflow attacks, null pointers, etc.

Requirements

SE_RTP.01	Run-time protection techniques as applicable to product architecture should be employed.
SE_RTP.02	Run-time protection techniques should be included to mitigate the impact of vulnerabilities.
SE_RTP.03	Run-time protection techniques should be included to protect executable code against memory space, buffer overflow attacks, and null pointers.

4.1.2.3 SE_VAR: Vulnerability Analysis and Response

Attribute Definition

Vulnerability analysis is the process of determining whether a product contains vulnerabilities and categorizing their potential severity.

Requirements

SE_VAR.01	Techniques and practices for vulnerability analysis shall be utilized. Some techniques include: code review, static analysis, penetration testing, white/black box testing, etc.
SE_VAR.02	The impact of published vulnerabilities to products and processes should be analyzed and mitigated.
SE_VAR.03	A process shall exist for governing notification of newly discovered and exploitable product vulnerabilities.
SE_VAR.04	Vulnerability analysis and response should feed into the processes for ongoing product development, product patching, and remediation.

4.1.2.4 SE_PPR: Product Patching and Remediation

Attribute Definition

A well-documented process exists for patching and remediating products. Priority is given to known severe vulnerabilities.

Requirements

SE_PPR.01	There shall be a well-documented process for patching and remediating products.
SE_PPR.02	There should be a process for informing an acquirer of notification and remediation mechanisms.
SE_PPR.03	Remediation of vulnerabilities shall be prioritized based on a variety of factors, including risk.
SE_PPR.04	Documented development and sustainment practices should be followed when implementing product remediation.

4.1.2.5 SE_SEP: Secure Engineering Practices

Attribute Definition

Secure engineering practices are established to avoid common engineering errors that lead to exploitable product vulnerabilities.

Requirements

SE_SEP.01	Secure coding practices shall be utilized to avoid common coding errors that lead to exploitable product vulnerabilities. For example, user input validation, use of appropriate compiler flags, etc.
SE_SEP.02	Secure hardware design practices (where applicable) shall be employed. For example, zeroing out memory and effective opacity.
SE_SEP.03	Training on secure engineering practices shall be provided to the appropriate personnel on a regular basis consistent with changing practices and the threat landscape.

4.1.2.6 SE_MTL: Monitor and Assess the Impact of Changes in the Threat Landscape

Attribute Definition

The threat landscape is monitored and the potential impacts of changes in the threat landscape are assessed on development/engineering practices, tools, and techniques.

Requirements

SE_MTL.01	Changes to the threat landscape should be monitored by periodically reviewing industry security alerts/bulletins.

SE_MTL.02	Changes to the development/engineering practices, tools, and techniques shall be assessed in light of changes to the threat landscape.
SE_MTL.03	The cause of product vulnerabilities shall be evaluated and appropriate changes to the development/engineering practices, tools, and techniques identified to mitigate similar vulnerabilities in the future.

4.2 Supply Chain Security

Trusted Technology Providers manage their supply chains through the application of defined, monitored, and validated supply chain processes. These processes, embodied in best practice requirements and recommendations, seek to ensure the security of the supply chain throughout the life cycle. In general, a technology supply chain attack is an attempt to disrupt the creation of goods by subverting the hardware, software, or configuration of a commercial product, prior to customer delivery (e.g., manufacturing, ordering, or distribution) for the purpose of introducing an exploitable vulnerability or perpetrating fraud through counterfeiting. The primary focus of the O-TTPS Supply Chain category of provider activities is to assure the integrity of the technology manufacturing/development and support processes. This is the second product life cycle category used to organize the requirements in this Standard.

4.2.1 SC: Supply Chain Security

The following sections contain the best practice requirements and recommendations primarily associated with the Supply Chain Security category of activities relating to the product life cycle.

4.2.1.1 SC_RSM: Risk Management

Attribute Definition

The management of supply chain risk around tainted and counterfeit components and products includes the identification, assessment, prioritization, and mitigation of corresponding business, technical, and operational risks.

Requirements

SC_RSM.01	Changes to the threat landscape should be monitored by periodically reviewing industry security alerts/bulletins.
SC_RSM.02	Supply chain risk identification, assessment, prioritization, and mitigation shall be conducted.
SC_RSM.03	The output of risk identification, assessment, and prioritization shall be addressed by a mitigation plan, which shall be documented.
SC_RSM.04	The output of risk identification, assessment, and prioritization shall be addressed by a mitigation plan, which shall be followed routinely.
SC_RSM.05	The mitigation plan should be reviewed periodically by practitioners, including management, and revised as appropriate.

SC_RSM.06	Supply chain risk management training shall be incorporated in a provider's organizational training plan, which shall be reviewed periodically and updated as appropriate.

4.2.1.2 SC_PHS: Physical Security

Attribute Definition

Physical security procedures are necessary to protect development assets and artifacts, manufacturing processes, the plant floor, and the supply chain.

Requirements

SC_PHS.01	Risk-based procedures for physical security shall be established and documented.
SC_PHS.02	Risk-based procedures for physical security shall be followed routinely.
SC_PHS.03	Risk-based procedures for physical security should be reviewed periodically by practitioners, including management, and revised as appropriate.

4.2.1.3 SC_ACC: Access Controls

Attribute Definition

Proper access controls are established for the protection of product-relevant intellectual property against the introduction of tainted and counterfeit components where applicable in the supply chain. Access controls can vary by type of intellectual property and over time, during the life cycle.

Requirements

SC_ACC.01	Access controls shall be established and managed for product-relevant intellectual property, assets, and artifacts. Assets and artifacts include controlled elements related to the development/manufacturing of a provider's product.
SC_ACC.02	Access controls established and managed for product-relevant intellectual property, assets, and artifacts shall be documented.
SC_ACC.03	Access controls established and managed for product-relevant intellectual property, assets, and artifacts shall be followed routinely.
SC_ACC.04	Access controls established and managed for product-relevant intellectual property, assets, and artifacts should be reviewed periodically by practitioners, including management, and revised as appropriate.
SC_ACC.05	Access controls established and managed for product-relevant intellectual property, assets, and artifacts shall employ the use of access control auditing.

4.2.1.4 SC_ESS: Employee and Supplier Security and Integrity

Attribute Definition

Background checks are conducted for employees and contractors whose activities are directly related to sensitive product supply chain activities.

A Provider has a set of applicable business conduct guidelines for their employee and supplier communities.

A Provider obtains periodic confirmation that suppliers are conducting business in a manner consistent with principles embodied in industry conduct codes, such as the Electronic Industry Citizenship Coalition (EICC) Code of Conduct.

Requirements

SC_ESS.01	Proof of identity shall be ascertained for all new employees and contractors engaged in the supply chain, except where prohibited by law.
SC_ESS.02	Background checks should be conducted for employees and contractors whose activities are directly related to sensitive product supply chain activities (within reason given local customs and according to local law).
SC_ESS.03	A set of business conduct guidelines applicable to its employees and contractors should exist, consistent with principles embodied in industry conduct codes such as the Electronic Industry Citizenship Coalition (EICC) Code of Conduct.
SC_ESS.04	Business should be conducted in a manner consistent with principles embodied in industry conduct codes, such as the Electronic Industry Citizenship Coalition (EICC) Code of Conduct.
SC_ESS.05	Periodic confirmation that suppliers are conducting business in a manner consistent with principles embodied in industry conduct codes, such as the Electronic Industry Citizenship Coalition (EICC) Code of Conduct, should be obtained.

4.2.1.5 SC_BPS: Business Partner Security

(This includes, for example, Suppliers, Integrators, Logistic Partners, Channel Partners, and Authorized Resellers.)

Attribute Definition

Relevant business partners follow the recommended supply chain security best practice requirements specified by the O-TTPS.

Periodic confirmation is requested that business partners are following the supply chain security best practices requirements specified by the O-TTPS.

Requirements

SC_BPS.01	Supply chain security best practices (e.g., O-TTPS) shall be recommended to relevant business partners.
SC_BPS.02	Legal agreements with business partners should reference applicable requirements for supply chain security practices (e.g., O-TTPS).
SC_BPS.03	The provider should periodically request confirmation that business partners are following the supply chain security best practice requirements specified by the O-TTPS.

4.2.1.6 SC_STR: Supply Chain Security Training

Attribute Definition

Personnel responsible for the security of supply chain aspects are properly trained.

Requirements

SC_STR.01	Training in supply chain security procedures shall be given to all appropriate personnel.

4.2.1.7 SC_ISS: Information Systems Security

Attribute Definition

Supply Chain information systems properly protect data through an appropriate set of security controls.

Requirements

SC_ISS.01	Supply chain data shall be protected through an appropriate set of security controls.

4.2.1.8 SC_TTC: Trusted Technology Components

Attribute Definition

Supplied components are evaluated to assure that they meet component specification requirements.

Suppliers follow supply chain security best practices with regard to supplied components (e.g., O-TTPS).

Requirements

SC_TTC.01	The quality of supplied components shall be assessed against the component specification requirements.

SC_TTC.02	Counterfeit components shall not knowingly be incorporated into products.
SC_TTC.03	Suppliers should be required to follow supply chain security best practices with regard to supplied components (e.g., O-TTPS).
SC_TTC.04	Vulnerability responses to affected supplied components should be jointly managed with the supplier.

4.2.1.9 SC_STH: Secure Transmission and Handling

Attribute Definition

Secure transmission and handling of assets and artifacts during delivery is needed to lower the risk of product tampering while in transit to their destination.

Requirements

SC_STH.01	Secure transmission and handling controls shall be established and documented.
SC_STH.02	Secure transmission and handling controls shall be designed to lower the risk of physical tampering with assets and artifacts that are physically transported.
SC_STH.03	Secure transmission and handling controls shall be designed to lower the risk of tampering with assets and artifacts that are electronically transmitted.
SC_STH.04	Secure transmission and handling controls shall be followed routinely.
SC_STH.05	Secure transmission and handling controls should be reviewed periodically by practitioners, including management, and revised as appropriate.
SC_STH.06	For assets and artifacts and related information that are considered to be high risk from the supply chain perspective, additional countermeasures, such as authenticity verification, should be employed.
SC_STH.07	Methods of verifying authenticity and integrity of products after delivery should be available.

4.2.1.10 SC_OSH: Open Source Handling

Attribute Definition

Open Source components are managed as defined by the best practices within the O-TTPS for Product Development/ Engineering methods and Secure Development/Engineering methods.

Requirements

SC_OSH.01	Open Source assets and artifacts should be managed as defined by the best practices within the O-TTPS for Product Development/Engineering methods and Secure Development/Engineering methods.
SC_OSH.02	In the management of Open Source assets and artifacts, components sourced shall be identified as derived from well-understood component lineage.

SC_OSH.03	In the management of Open Source assets and artifacts, components sourced shall be subject to well-defined acceptance procedures that include asset and artifact security and integrity before their use within a product.
SC_OSH.04	For such sourced components, responsibilities for ongoing support and patching shall be clearly understood.

4.2.1.11 SC_CTM: Counterfeit Mitigation

Attribute Definition

Practices are deployed to manufacture, deliver, and service products that do not contain counterfeit components.

Practices are deployed to control the unauthorized use of scrap from the hardware manufacturing process.

Requirements

SC_CTM.01	Instances of counterfeit activity relating to products shall be reviewed and an appropriate response sent.
SC_CTM.02	Proper disposal procedures upon end of life should be employed (e.g., clearing data from hard drives, rendering a PCB non-functional, etc.) to protect from re-use in counterfeit product.
SC_CTM.03	Practices should be deployed to preclude the unauthorized (counter-indicated) use of scrap from the hardware manufacturing process.
SC_CTM.04	Techniques shall be utilized as applicable and appropriate to mitigate the risk of counterfeiting, such as security labeling and scrap management techniques.

4.2.1.12 SC_MAL: Malware Detection

Attribute Definition

Practices are employed that mitigate as much as practical the inclusion of malware in components received from suppliers and components or products delivered to customers or integrators.

Requirements

SC_MAL.01	One or more up-to-date malware detection tools shall be deployed as part of the code acceptance and development processes.
SC_MAL.02	Malware detection techniques shall be used before final packaging and delivery (e.g., scanning finished products and components for malware using one or more up-to-date malware detection tools).

Glossary

The following terms and acronyms are used in this Standard:

Accreditation Program
: A process in which certification of competency or credibility is provided. As used in this Standard, it is a process that a supplier goes through to certify that they meet the requirements of an Open Trusted Technology Provider Standard (O-TTPS).

Acquirer
: One who procures hardware and software products and services to create solutions that meet their customers' requirements.

Artifact
: Something that results from applying a process.

Asset
: Anything you can use that is considered a thing of value (e.g., tool).

Backdoor
: An intentional and undisclosed mechanism (to the customer/user) in a product, service, or facility which is intended to provide access to assets and artifacts by an unauthorized party.

Best Practice
: Provides a clear description of a set of tried and tested processes, procedures, and guidelines that, when practically applied to an operation, brings a business advantage.

Certification/Accreditation Authority
: Provides certification and/or testing services, especially those involved with conformance certification and/or testing.

Component Supplier
: Entity that supplies components, typically as business partners to providers.

Configuration Management
: A formal process which ensures the proper management, control, and tracking of change to product development and manufacturing assets and artifacts.

Conformance Assessment
: The act of determining the consistency of an implementation to a specification, or the adherence of a business operation to a best practice or process definition.

Contractors/System Integrators
: Provide services and solutions to customers; typically used on large projects that deal with multiple providers.

COTS
: Commercial Off-the-Shelf hardware and software.

Counterfeit Product
: A product that is produced other than by, or for, the provider, or is supplied to the provider by other than a provider's authorized channel and is presented as being legitimate even though it is not.

Development Method
: System (or Software) Development Life Cycle (SDLC) development-based method. Applicable to both hardware and software-based products.

Downstream
: Any entity that is further down the supply chain process from the subject; i.e., the acquirer is downstream from the integrator (see Upstream).

Engineering Method
: Method that is focused on manufacturing or development processes and practices; for products with significant hardware-based technology components (chips, firmware, systems, etc.).

Framework
: Defines a set of structured processes and templates that facilitates solving a complex problem. As used in this Standard, a set of best practices identified by a cross-industry forum which, if used by a technology vendor, may allow a government or commercial enterprise customer to consider the vendor's products as more secure and trusted.

Grey Market
: Distribution channels which, while legal, are unofficial, unauthorized, or unintended by the original manufacturer.

ICT
: Information and Communications Technology.

Integrator
: A third-party organization that specializes in combining products from several suppliers to produce systems for a customer.

Integrity
: The condition of not being marred or violated; unimpaired or uncorrupted condition; original perfect state; soundness.[2]

ISO
: International Organization for Standardization.

Legitimate Product
: The item is produced by the provider and is acquired through a provider's authorized channel.

Life Cycle
: A progression through a series of differing stages of development. Commonly referred to as System Development Life Cycle (SDLC). The course of events that brings a new product into existence and follows its growth into a mature product and into eventual disposal.

May
: Refer to Section 1.3 (Terminology) for definition. Refer to the introduction to Chapter 4 for context.

[2] This definition is aligned with ISO/IEC 27000:2009.

Mitigation	Any action, device, procedure, technique, or any other measure that reduces the vulnerability or risk.
OEM	Original Equipment Manufacturer.
Open CA	The Open Group IT Architect Certification Program.
Open Source	Generically, the term "Open Source" refers to a program in which the source code is available to the general public for use and/or modification from its original design free-of-charge; i.e., open. Open Source code is typically created as a collaborative effort in which programmers improve upon the code and share the changes within the community. Open Source sprouted in the technological community as a response to proprietary software owned by corporations.[3]
OSS	Open Source Software – software that is developed collaboratively using an open (visible) development process.
OTTF	The Open Group Trusted Technology Forum. A global standards initiative to provide a collaborative, open environment for technology companies, customers, government, and supplier organizations to create and promote guidelines for manufacturing, sourcing, and integrating trusted, secure technologies.
O-TTPF	Open Trusted Technology Provider Framework (Framework). Initially released as a White Paper in February 2011, serves as the basis for the work defined here, future updates, and additional standards. The Framework is a compendium of organizational guidelines and best practices that if implemented enhance the security and integrity of Commercial Off-the-Shelf (COTS) Information and Communication Technology (ICT) products throughout the entire product life cycle, including the supply chain aspects of that life cycle. The content of the Framework is the result of industry collaboration and research as to the contemporary practical.
O-TTPS	A standard established by consensus within the OTTF and approved through The Open Group Company Review process that provides a set of organizational commercial requirements that enhance the security of the global supply chain and the integrity of COTS ICT products. It provides a set of guidelines and best practice requirements and recommendations that help assure against tainted and counterfeit products throughout the COTS ICT product life cycle encompassing the following phases: design, sourcing, build, fulfillment, distribution, sustainment, and disposal.
Product Life Cycle Categories	The two major categories of activities in the product life cycle that this Standard covers are: Category 1: Technology Development – focuses on two major best practice

[3] Source: Wikipedia.

sub-categories: product development/engineering and secure development/engineering, and is typically under the direct control of the provider.

Category 2: Supply Chain Security – focuses on best practices with respect to the supply chain throughout the following product life cycle phases: design, sourcing, build, fulfillment, distribution, sustainment, and disposal. Here the provider's best practices control the point of intersection at the various nodes, and rely on the provider's influence and contracts with the supplier.

Product Sustainment Management
: Product support, release maintenance, and defect management are offered to customers while the product is generally available.

Providers
: As used in this Standard, a midstream vendor developing products and managing the supply chain to provide acquirers and integrators with trustworthy products.

Risk
: An event or condition that has a potentially negative impact and the possibility that such an event will occur and adversely affect an entity's assets and artifacts, activities, and operations.

Risk Management
: The process concerned with the identification, measurement, control, and mitigation of risk.

Shall
: Refer to Section 1.3 (Terminology) for definition. Refer to the introduction to Chapter 4 for context.

Should
: Refer to Section 1.3 (Terminology) for definition. Refer to the introduction to Chapter 4 for context.

Standards Body
: Any organization whose primary activities are developing, coordinating, promulgating, revising, amending, re-issuing, interpreting, or otherwise producing standards that are intended to address the needs of some relatively wide base of affected adopters.

Suppliers
: An upstream vendor who develops hardware or software components for providers.

Supply Chain
: A set of organizations, people, activities, information, and resources for creating and moving a product or service (including its sub-elements) from suppliers through to customers. One of the two major categories in this standard is Supply Chain Security.

Supply Chain Attack (general)
: An attempt to disrupt the creation of goods by subverting the hardware, software, or configuration of a commercial product, prior to customer delivery (e.g., manufacturing, ordering, or distribution) for the purpose of introducing an exploitable vulnerability.

Supply Chain Risk Management
: The identification, assessment, prioritization, and mitigation of business, technical, and physical risks as they pertain to the manufacturing process including the use of third-party components and services in addition to the delivery of the product to the end user.

Supply Chain Security
: The manufacturing and/or development process performs its intended function in an unimpaired manner, free from deliberate or inadvertent manipulation. Extends the NIST definition [NIST 800-12].

System Life Cycle
: The phases of a system or proposed system that address its existence from inception to retirement.

Tainted Product
: A product that is produced by the provider and is acquired through a provider's authorized channel but has been tampered with maliciously.

  Note: All instances, within this standard, of the use of the words: taint, tainted, tainting refer to maliciously taint, maliciously tainted, and maliciously tainting, respectively.

Technology Provider
: See Provider.

Technology Supply Chain
: The manufacturing and/or development process used to produce and deliver hardware or software technology products and their configuration.

Technology Supply Chain Attack
: An attack that subverts the hardware, software, or configuration of a product, prior to customer delivery, for the purpose of introducing an exploitable vulnerability.

Technology-neutral
: An approach whereby the decision to use technology required to meet a stated need is free of any bias.

Threat
: The intention and capability of an adversary to undertake actions that would be detrimental through disruption of processes or subversion of knowledge.

Trusted Technology Provider
: An organization that has been successfully accredited as being conformant to the requirements defined in this Open Trusted Technology Provider Standard (O-TTPS).

Upstream
: Any entity who is further up the supply chain process from the subject; i.e., vendors who supply component parts or solutions (software or hardware) to providers or integrators (see Downstream).

Vendor
: Builds products or components (hardware or software).

Vendor-neutral
: An approach whereby the decision to use a vendor required to meet a stated technology need is free of any bias.

Vulnerability
: A weakness in the design, implementation, or operation of an asset, artifact, system, or network that can be exploited.

Vulnerability Analysis
: The process of determining whether a product contains vulnerabilities and categorizing their potential severity.