INTERNATIONAL STANDARD

ISO/IEC 20243-1

Second edition
2023-11

Information technology — Open Trusted Technology Provider™ Standard (O-TTPS) —

Part 1: Requirements and recommendations for mitigating maliciously tainted and counterfeit products

Reference number
ISO/IEC 20243-1:2023(E)

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

Contents

Page

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular, the different approval criteria needed for the different types of document should be noted (see www.iso.org/directives or www.iec.ch/members_experts/refdocs).

ISO and IEC draw attention to the possibility that the implementation of this document may involve the use of (a) patent(s). ISO and IEC take no position concerning the evidence, validity or applicability of any claimed patent rights in respect thereof. As of the date of publication of this document, ISO and IEC had not received notice of (a) patent(s) which may be required to implement this document. However, implementers are cautioned that this may not represent the latest information, which may be obtained from the patent database available at www.iso.org/patents and https://patents.iec.ch. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT), see www.iso.org/iso/foreword.html. In the IEC, see www.iec.ch/understanding-standards.

This document was prepared by The Open Group [as Open Trusted Technology Provider Standard (O-TTPS) V1.2, Part 1: Requirements and Recommendations] and drafted in accordance with its editorial rules. It was adopted, under the JTC 1 PAS procedure, by Joint Technical Committee ISO/IEC JTC 1, *Information technology*.

This second edition cancels and replaces the first edition (ISO/IEC 20243-1:2018), which has been technically revised.

The main changes are as follows:

— Wording was changed throughout the document, including in beginning materials, attribute definitions and requirements, as necessary to improve clarity and/or concision.

— The definition of “component” has been clarified to include both hardware and software.

— A definition for “security-critical” has been added.

— PD_DES.01 has become a mandatory requirement.

— PD_CFM.04 has become a mandatory requirement.

— The attribute definition of PD_QAT has been clarified.

— The attribute definition of PD_PSM has been clarified.

— The SE_VAR requirements have been largely reworked and reorganized, with a new mandatory requirement being added and several existing requirements becoming mandatory.

— SE_PPR.02 has become a mandatory requirement.

— SE_PPR.04 has become a mandatory requirement.

— SC_RSM.05 has become a mandatory requirement.

— SC_ACC.04 has become a mandatory requirement.

— SC_ESS.02 has become a mandatory requirement.

— SC_ESS.03 has become a mandatory requirement.

— SC_ESS.04 has been completely rewritten and has become a mandatory requirement.

— SC_BPS.02 has become a mandatory requirement.

— The SE_STH requirements have been largely reworked and reorganized, with a new requirement being added and an existing requirement becoming mandatory.

— SC_CTM.02 has been heavily revised and has become a mandatory requirement.

— SC_MAL.02 has been heavily revised and has become a mandatory requirement

A list of all parts in the ISO/IEC 20243 series can be found on the ISO and IEC websites.

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html and www.iec.ch/national-committees.

Preface

The Open Group

The Open Group is a global consortium that enables the achievement of business objectives through technology standards. With more than 870 member organizations, we have a diverse membership that spans all sectors of the technology community – customers, systems and solutions suppliers, tool vendors, integrators and consultants, as well as academics and researchers.

The mission of The Open Group is to drive the creation of Boundaryless Information Flow™ achieved by:

— Working with customers to capture, understand, and address current and emerging requirements, establish policies, and share best practices

— Working with suppliers, consortia, and standards bodies to develop consensus and facilitate interoperability, to evolve and integrate specifications and open source technologies

— Offering a comprehensive set of services to enhance the operational efficiency of consortia

— Developing and operating the industry's premier certification service and encouraging procurement of certified products

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 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/library.

This Document

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

This document is Part 1 of the Open Trusted Technology Provider Standard (O-TTPS). It 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 document: the O-TTPF (Framework) and the O-TTPS (Standard).

The O-TTPF (Framework): The O-TTPF is an evolving compendium of organizational guidelines and best practices relating to the integrity of Commercial Off-The-Shelf (COTS) Information and Communications Technology (ICT) products and the security of the supply chain throughout the entire product lifecycle.

An early version of the O-TTPF was published as a White Paper in February 2011, revised in November 2015, and has since been updated and published as a Guide in September 2021. The O-TTPF serves as the basis for the O-TTPS, future updates, and additional standards. The content of the O-TTPF 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 O-TTPF 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. Part 1 of the O-TTPS (this document) provides a set of guidelines, requirements, and recommendations that help assure against maliciously tainted and counterfeit products throughout the COTS ICT product lifecycle encompassing the following phases: design, sourcing, build, fulfillment, distribution, sustainment, and disposal.

The O-TTPS, Part 2: Assessment Procedures for the O-TTPS provides assessment procedures that may be used to demonstrate conformance with the requirements provided in Clause 6 of this document.

Using the guidelines documented in the O-TTPF 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 by releasing addenda to address specific threats or market needs.

The O-TTPS is aimed at enhancing the integrity of COTS ICT products and helping customers to manage sourcing risk. The authors 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

The O-TTPS 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 O-TTPS in their organizations. Additionally, acquirers and customers can begin recommending the adoption of the O-TTPS to their providers and integrators.

Trademarks

ArchiMate, DirecNet, Making Standards Work, Open O logo, Open O and Check Certification logo, Platform 3.0, The Open Group, TOGAF, UNIX, UNIXWARE, and the Open Brand X logo are registered trademarks and Boundaryless Information Flow, Build with Integrity Buy with Confidence, Commercial Aviation Reference Architecture, Dependability Through Assuredness, Digital Practitioner Body of Knowledge, DPBoK, EMMM, FACE, the FACE logo, FHIM Profile Builder, the FHIM logo, FPB, Future Airborne Capability Environment, IT4IT, the IT4IT logo, O-AA, O-DEF, O-HERA, O-PAS, Open Agile Architecture, Open FAIR, Open Footprint, Open Process Automation, Open Subsurface Data Universe, Open Trusted Technology Provider, OSDU, Sensor Integration Simplified, SOSA, and the SOSA logo are trademarks of The Open Group.

All other brands, company, and product names are used for identification purposes only and may be trademarks that are the sole property of their respective owners.

Introduction

Part 1 of the 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 document, 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 document is a commitment to using specific methodologies to assure the integrity of their hardware or software Commercial Off-The-Shelf (COTS) Information and Communications Technology (ICT) products. This document is detailed and prescriptive enough to be useful in raising the bar for all providers and lends itself to the accompanying certification process that provides assurance that it is being followed in a meaningful and repeatable manner.

Part 1 of the O-TTPS (this document) 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 lifecycle. This version of the O-TTPS addresses threats related to maliciously tainted and counterfeit products.

The provider's product lifecycle includes the work it does designing and developing products, as well as the supply chain aspects of that lifecycle, collectively extending through the following phases: design, sourcing, build, fulfillment, distribution, sustainment, and disposal. While this document 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 this document 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 document, are defined as:

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

2. Counterfeit product – the product is produced other than by, or for, the provider, or it 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 document, of the use of the words: taint, tainted, tainting, refer to malicious taint, maliciously tainted, and malicious tainting, respectively.

Trusted Technology Providers manage their product lifecycle, 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 document. 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.

Information technology — Open Trusted Technology Provider™ Standard (O-TTPS) — Mitigating maliciously tainted and counterfeit products —

Part 1: Requirements and recommendations

1 Scope

This document is focused on the security of the supply chain *versus* the business management aspects of the supply chain. This document 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 lifecycle 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 document 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.

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

For this version of the O-TTPS, the following elements are considered out of scope:

— This document does not focus on guidelines, requirements, and recommendations for the acquirer; the OTTF is considering addressing this area in a separate, complementary publication, such as a Guide.

  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 document 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 Guide.

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

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

1.1 Conformance

The Open Group has developed and maintains conformance criteria, assessment procedures, and a Certification Policy and Program for the O-TTPS as a useful tool for all constituents with an interest in supply chain security.

The conformance requirements and assessment procedures are available in the O-TTPS, Part 2: Assessment Procedures for the O-TTPS.

Certification provides formal recognition of conformance to the O-TTPS, which allows:

— Providers and practitioners to make and substantiate clear claims of conformance to the O-TTPS

— Acquirers to specify and successfully procure from providers who conform to the O-TTPS

1.2 Future Directions

The OTTF intends to address possible additional threats and risks with best practice requirements and recommendations in a future version.

The OTTF intends to offer additional guidance for different classes of Trusted Technology Providers seeking certification against this document.

2 Normative references

There are no normative references in this document.

3 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

Shall	Indicates an absolute, mandatory requirement that has to be implemented in order to conform to this document 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, and if implemented would represent a non-conformity. 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 O-TTPS, 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.

Throughout this document, the term O-TTPS is used when referring to The Open Trusted Technology Provider Standard.

3.1
Acquirer
One who procures hardware and software products and services to create solutions that meet their customers' requirements.

3.2
Artifact
Something that results from applying a process.

3.3
Asset
Anything you can use that is considered a thing of value (e.g., tool).

3.4
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.

3.5
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.

3.6
Certification Authority
Provides certification and/or testing services, especially those involved with conformance certification and/or testing.

3.7
Certification Program
A process in which certification of competency or credibility is provided. As used in this document, it is a process that a supplier goes through to certify that they meet the requirements of the Open Trusted Technology Provider Standard (O-TTPS).

3.8
Component
Refers to either hardware or software; for hardware, it refers to any physical, cyber-active element, and for software, it refers to any module or executable within a system or application.

3.9
Component Supplier
Entity that supplies components, typically as business partners to providers.

3.10
Configuration Management
A formal process which ensures the proper management, control, and tracking of change to product development and manufacturing assets and artifacts.

3.11
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.

3.12
Contractors/System Integrators
Provide services and solutions to customers; typically used on large projects that deal with multiple providers.

3.13
COTS
Commercial Off-The-Shelf hardware and software.

3.14
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.

3.15
Development Method
System (or Software) Development Life Cycle (SDLC) development-based method. Applicable to both hardware and software-based products.

3.16
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).

3.17
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.).

3.18
Framework
Defines a set of structured processes and templates that facilitates solving a complex problem. As used in this document, 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.

3.19
Grey Market
Distribution channels which, while legal, are unofficial, unauthorized, or unintended by the original manufacturer.

3.20
ICT
Information and Communications Technology.

3.21
IEC
International Electrotechnical Commission.

3.22
Integrator
A third-party organization that specializes in combining products from several suppliers to produce systems for a customer.

3.23
Integrity
The condition of not being marred or violated; unimpaired or uncorrupted condition; original perfect state; soundness.

Note 1 to entry: This definition is aligned with ISO/IEC 27000:2009.

3.24
ISO
International Organization for Standardization.

3.25
Legitimate Product
The item is produced by the provider and is acquired through a provider's authorized channel.

3.26
Lifecycle
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.

3.27
Mitigation
Any action, device, procedure, technique, or any other measure that reduces the vulnerability or risk.

3.28
ODM
Original Design Manufacturer.

3.29
OEM
Original Equipment Manufacturer.

3.30
Open CA
The Open Group IT Architect Certification Program.

3.31
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.

[SOURCE: Wikipedia]

3.32
OSS
Open Source Software – software that is developed collaboratively using an open (visible) development process.

3.33
OTTF
The Open Group Open 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.

3.34
O-TTPF
Open Trusted Technology Provider Framework. Initially released as a White Paper in February 2011, revised in November 2015, and updated and published as a Guide in September 2021 (see Bibliography [5]), it serves as the basis for the work defined here, future updates, and additional standards. The O-TTPF 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 Communications Technology (ICT) products throughout the entire product lifecycle, including the supply chain aspects of that lifecycle. The content of the O-TTPF is the result of industry collaboration and research as to the contemporary practical.

3.35
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 lifecycle encompassing the following phases: design, sourcing, build, fulfillment, distribution, sustainment, and disposal.

3.36
Product Lifecycle Categories
The two major categories of activities in the product lifecycle covered in this document are:

— Category 1: Technology Development – focuses on two major best practice 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 lifecycle 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

3.37
Product Sustainment Management
Product support, release maintenance, and defect management are offered to customers while the product is generally available.

3.38
Providers
As used in this document, a midstream vendor developing products and managing the supply chain to provide acquirers and integrators with trustworthy products.

3.39
PSIRT
Product Security Incident Response Team.

3.40
RBA
Responsible Business Alliance.

3.41
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.

3.42
Risk Management
The process concerned with the identification, measurement, control, and mitigation of risk.

3.43
Security-Critical
A business partner that provides or a process that uses a logic-bearing or software component for a product; encompasses all aspects of security, including physical, cyber, and supply chain security.

3.44
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.

3.45
Supplier
An upstream vendor who develops hardware or software components for providers.

3.46
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 document is Supply Chain Security.

3.47
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.

3.48
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.

3.49
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 SP 800-12].

3.50
System Lifecycle
The phases of a system or proposed system that address its existence from inception to retirement.

3.51
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 1 to entry: All instances, within this document, of the use of the words: taint, tainted, tainting refer to malicious taint, maliciously tainted, and malicious tainting, respectively.

3.52
Technology Provider
See Provider.

3.53
Technology Supply Chain
The manufacturing and/or development process used to produce and deliver hardware or software technology products and their configuration.

3.54
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.

3.55
Technology-neutral
An approach whereby the decision to use technology required to meet a stated need is free of any bias.

3.56
Threat
The intention and capability of an adversary to undertake actions that would be detrimental through disruption of processes or subversion of knowledge.

3.57
Trusted Technology Provider
An organization that has been successfully certified as being conformant to the requirements defined in the Open Trusted Technology Provider Standard (O-TTPS).

3.58
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).

3.59
VAR
Value-Add Reseller.

3.60
Vendor
Builds products or components (hardware or software).

3.61
Vendor-neutral
An approach whereby the decision to use a vendor required to meet a stated technology need is free of any bias.

3.62
Vulnerability
A weakness in the design, implementation, or operation of an asset, artifact, system, or network that can be exploited.

3.63
Vulnerability Analysis
The process of determining whether a product contains vulnerabilities and categorizing their potential severity.

4 Business Context and Overview

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

4.1 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, an understanding is needed of the extent of the global supply chain by looking at an operational scenario.

4.1.1 Operational Scenario

Figure 1: Constituents 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.

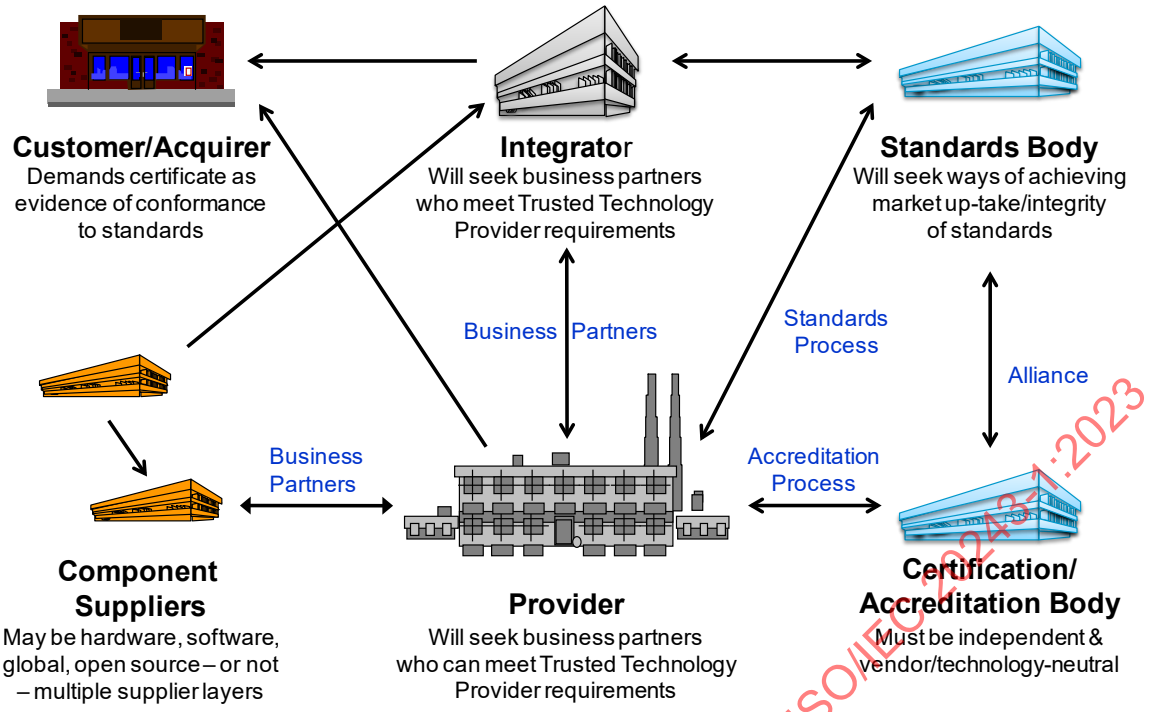

Figure 1 — Constituents

Table 1: O-TTPS Constituents and their Roles describes the roles of these constituents in this document.

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.

Constituent	Role Played
Vendor	Synonymous with provider.
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 process with certification bodies. Requests that their suppliers follow the O-TTPS and have been certified 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 bodies.
Certification 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 process with vendors.

4.2 Business Rationale

The following clauses provide the business rationale for the O-TTPS by presenting the business drivers and benefits. Clause 4.3 provides more context on what this document can and cannot reasonably cover.

4.2.1 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, certifying providers who follow those best practices, and knowing how to identify trustworthy products that were built by Trusted Technology Providers.

4.2.2 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 OTTF is intended to facilitate the evolution of the O-TTPF 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 maintains the O-TTPS Certification Program that allows providers who meet the O-TTPS requirements and recommendations to become certified and acknowledged on a public certification registry, so that customers from industry and government can buy from those Trusted Technology Providers with increased confidence.

The work of the OTTF 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 brought to the table their own best practices and created a composite set of best practice requirements and recommendations to be codified in this and future versions. The OTTF work is notable in representing consensus for commercially reasonable best practices from industry in addressing the threats in focus.

The O-TTPS is 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, is a major benefit for global providers and customers, including governments.

4.3 Recognizing the COTS ICT Context

It is important in defining this set 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 the O-TTPS. 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 the O-TTPS 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 Clause 5: O-TTPS – Tainted and Counterfeit Risks of this document. A focus on best practices in these risk areas can 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 document does provide best practice requirements that helps 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 document.

Last, even though “tainting” is rightly a focus area of this document, 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 document does identify best practice requirements and recommendations in those areas of risk. If followed in conjunction with the other best practice requirements identified in this document, they will help to reduce the possibility of malicious code being introduced as the product progresses throughout its lifecycle and measurably further the goal of an improved global market encompassing trustworthy suppliers and trustworthy products.

4.4 Overview

This clause provides overviews of the O-TTPF and O-TTPS, and adds findings from the Standards Harmonization Work Stream of the OTTF.

4.4.1 O-TTPF Overview

This clause addresses the O-TTPF for reference purposes only and to provide context. This document addresses mitigating tainted and counterfeit products in subsequent clauses.

[1)] For support of this premise, refer to the 2007 Report of the Defense Science Board Task Force on Mission Impact of Foreign Influence on DoD Software and the July 2021 Press Release from ENISA on Understanding the Increase in Supply Chain Security Attacks (see Bibliography [8]). It is not currently a solvable problem, or even a problem for which there are acceptable mitigation techniques.

The O-TTPF organizes best practices into the following four categories:

1. Product Development/Engineering Method
2. Secure Development/Engineering Method
3. Supply Chain Security Method
4. 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 the O-TTPS. The concept of a Product Evaluation Method as referenced in the O-TTPF is focused specifically on product security. This version, 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 document have been derived from and informed by the broad O-TTPF method categories, only those requirements and recommendations that pertain directly to the two specific risks identified in Clause 5 – namely, tainted and counterfeit products – are set forth in this document.

The publicly available O-TTPF can be found in the O-TTPF Guide (see Bibliography [5]).

4.4.2 O-TTPS Overview

In releasing standards based on the O-TTPF to the global community, the OTTF decided to scope this version of the O-TTPS to best practice requirements and recommendations for reducing the threats and mitigating the risks associated with tainted and counterfeit products. Best practice requirements and recommendations in this document are presented in two categories of product lifecycle activities:

1. Technology Development
2. Supply Chain Security

4.4.3 Relationship with Other Standards

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

5 O-TTPS – Tainted and Counterfeit Risks

This clause highlights certain risks associated with tainted and counterfeit COTS ICT products. The following clause, Clause 6, specifies the requirements and recommendations of the O-TTPS that, when implemented by Trusted Technology Providers, are designed to reduce those risks.

As defined in the Introduction, 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: Threat Mapping illustrates this dimension for both tainted and counterfeit products in relation to some of the more serious risks, specifically:

1. **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)

2. **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)

3. **Unauthorized Configuration**: the introduction of potentially dangerous changes to control settings, attack surface, etc.

4. **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

5. **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: Threat Mapping, 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

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

This clause defines the requirements and recommendations relating to tainted and counterfeit product risks for this version of the O-TTPS.

NOTE It is important to understand that all of the requirements and recommendations listed in the tables in this clause are specified using prescriptive terms (e.g., shall, should, may); for definitions of these terms, please refer to the definitions in Clause 3. For reasons of consistency, these terms are equivalent to the corresponding ISO definitions.

The O-TTPS is described in terms of the provider’s product lifecycle. 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 COTS ICT product from its inception to proper disposal at end-of-life. These provider practices are divided into two basic categories of product lifecycle activities, as described in Clause 4.4.2:

— **Technology Development**

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.

— **Supply Chain Security**

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 lifecycle. 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 lifecycle 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 lifecycle are depicted in Figure 2: Product Lifecycle – Categories and Activities:

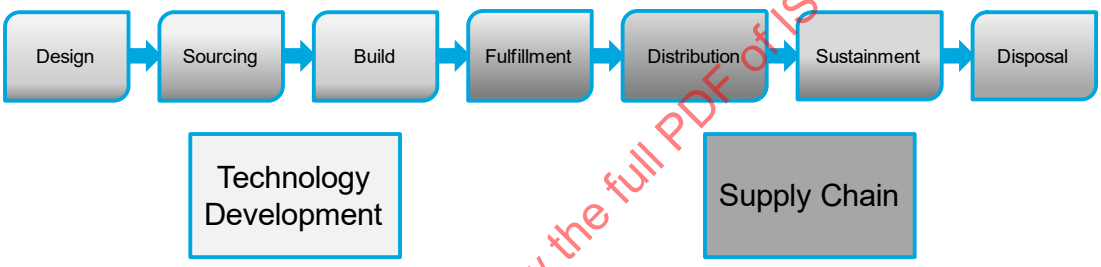

Figure 2 — Product Lifecycle – Categories and Activities

For structural purposes, in Clauses 6.1 and 6.2, the requirements and recommendations are delineated in separate clauses 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 clauses include the prescriptive requirements and recommendations for this document. The requirements are focused on the two identified threats. Some are highly correlated to the specific threats; others are more foundational but considered essential.

6.1 Technology Development

For purposes of addressing tainted and counterfeit products, the Technology Development category of the product lifecycle reflects the following methods, which are referred to in Clause 6.1.1 and Clause 6.1.2:

— **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.

— **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.

6.1.1 PD: Product Development/Engineering Method

The following clauses contain the best practice requirements and recommendations primarily associated with the Technology Development category of activities relating to the Product Development/Engineering Method.

6.1.1.1 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 shall be tracked as part of the design process.

6.1.1.2 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 shall 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.

6.1.1.3 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 lifecycle.

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 lifecycle.

6.1.1.4 PD_QAT: Quality and Test Management

Attribute Definition

Quality and test management is practiced as part of the product development/engineering lifecycle. Changes in the product are validated as part of the nominal process of product development/engineering.

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 lifecycle (i.e., at appropriate stages).

6.1.1.5 PD_PSM: Product Sustainment Management

Attribute Definition

Product support, release maintenance (i.e., changes/updates to an existing product), and defect management are product sustainment services managed throughout the lifecycle of the product and made 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.

6.1.2 SE: Secure Development/Engineering Method

The following clauses contain the best practice requirements and recommendations primarily associated with the Technology Development category of activities relating to the Secure Development/Engineering Method.

6.1.2.1 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.

6.1.2.2 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 unreleased memory space, buffer overflow attacks, null pointers, etc.

6.1.2.3 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	A process shall exist for governing notification of newly discovered and exploitable product vulnerabilities.
SE_VAR.03	The impact of published vulnerabilities to dependent products and processes (i.e., products and processes on which the organization depends to produce its products; these may be the sub-components of the final product or tools used in product development) should be analyzed and mitigated.
SE_VAR.04	The impact of published vulnerabilities to the product of the organization being assessed for conformance shall be analyzed and mitigated.
SE_VAR.05	Vulnerability analysis and response (PSIRT) shall feed into the processes for ongoing product development, product patching, and remediation.

6.1.2.4 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 shall be a process for informing an acquirer of mechanisms for notification and remediation.
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 (e.g., ensuring updates to the project are managed, new capabilities are provided, and continuous roll-forward updates occur) shall be followed when implementing product remediation.

6.1.2.5 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, secure boot, zeroing out memory, effective opacity, etc.
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.

6.1.2.6 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.