

Securing Global IT Supply Chains and IT Products by
Working with Open Trusted Technology Provider™
Accredited Companies

The Open Group Launches Accreditation Program

for

Organizations who Conform to the

Open Trusted Technology Provider™ Standard (O-TTPS)

The Challenge...

Global Supply Chain security for COTS products

Commercial Off the Shelf Products are developed and used globally

COTS products rely on components that are often globally sourced

COTS products are integrated into Critical Infrastructure, Government systems and Commercial solutions

THREATS

Counterfeit product

Maliciously tainted

Tainted

Insiders

Obsolescence

Many others ...

The OTTF

- ❑ **Government-industry roundtable discussion in 2009**
 - Initiated by DoD AT&L(SE), DoD-CIO and The Open Group
- ❑ **Government raised these issues**
 - Moving *from* high assurance customized solutions *to* Commercial Off The Shelf (COTS) Information Communication Technology (ICT)
 - Need to confidently identify trusted COTS ICT products/providers
- ❑ **Government recommendation**
 - **Establish consensus on best of breed best practices** based on industry experience to create a standard that enables all providers to conform to those best practices when building products.
 - **Create an accreditation program brand** that identifies trusted technology providers who conform to the standard
- ❑ **Response to the recommendation – the OTTF**
 - Providers, integrators, government agencies, third party labs from around the globe responded to the recommendation

The O-TTIPS



The first version of the O-TTIPS addresses the two threats that have been identified as the most pressing:

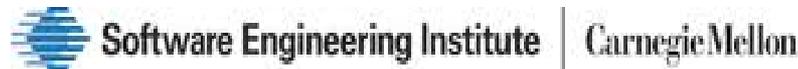
- Maliciously Tainted
- Counterfeit Products

The Open Group Trusted Technology Forum

A global industry-led initiative defining best practices for secure engineering and supply chain integrity so that you can “*Build with Integrity and Buy with Confidence*™”



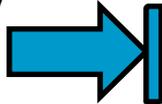
Booz | Allen | Hamilton



OTTF Milestones and Time Frames



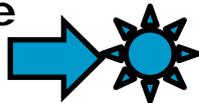
Early Industry Collaboration



Forum Launched



Framework White Paper Published



Standard Development: Snapshot => Publish V 1.0

Define Conformance Criteria, Conduct Pilot Program

Define & Approve O-TTPS Accreditation Program

Implement and Launch Public O-TTPS Accreditation Program

O-TTPS v. 1.0 published April 2013

Conducted Pilot of the O-TTPS Accreditation

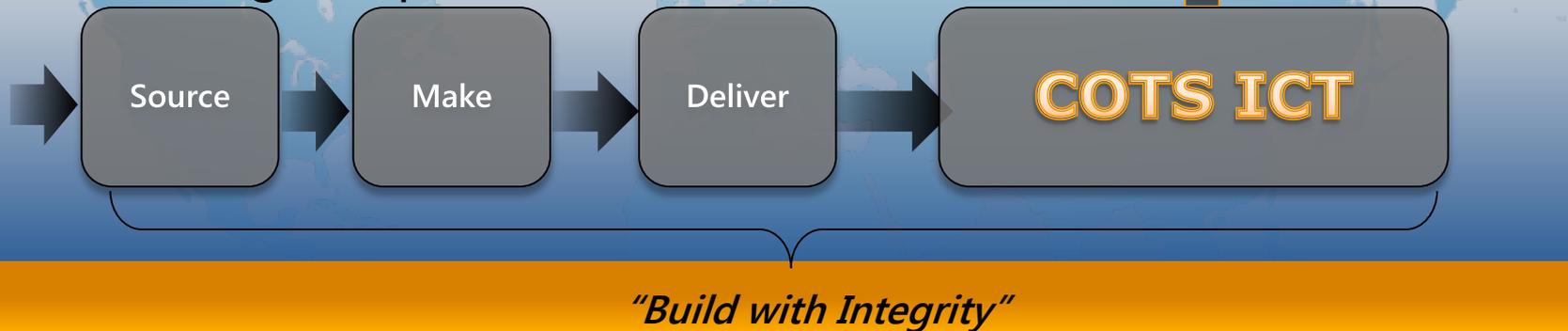
Feb 3, 2014 Announce:
1. Public Launch of Accreditation Program
2. First Accredited Open Trusted Technology Provider™

The OTTF Roadmap 2Q 2014 – 2Q 2015

<u>Deliverables</u>	Amsterdam 2Q2014	Boston 3Q2014	London 4Q2014	San Diego 1Q2015	Spain 2Q2015
O-TTPS - version 1.1.	Develop	Review & Publish			
O-TTPS 1.1 ISO PAS Submission	Develop	Request to ISO to accept PAS Submission	ISO Review	ISO Review	ISO Ballot (Projected Time Frame)
O-TTPS 1.1. Translation (Simplified Chinese)		Develop	Review & Publish		
O-TTPS Assessment Procedures – V 1.1		Develop	Review & Publish		
O-TTPS Mapping to other standards: CC, NIST, ... Ongoing		Develop	Review & Publish CC Mapping	Develop	Develop
O-TTPS 2.0			Develop	Develop	Develop

The O-TTPS Program Responds to the Challenge

Product certification is not enough - need assurance throughout that best practices are being followed when building the products.



Challenge: Commercial Off-the-Shelf (COTS) Information and Communication Technology (ICT) leverage a Global Supply Chain

Response: O-TTPS Standard and Accreditation Program

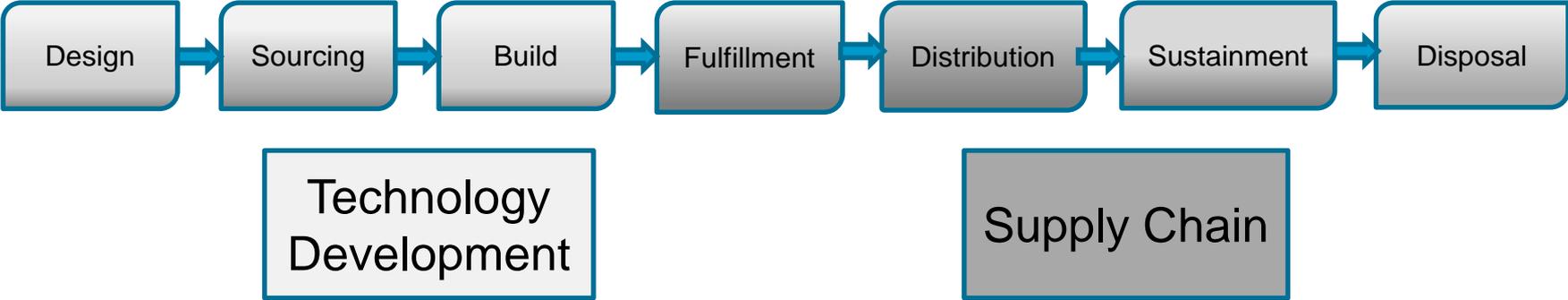
***Requiring Full Product Life Cycle Approach
Offering a Standard for Best Practices for all Constituents in the Chain
Providing Accreditation to Help Assure Conformance to the Standard***

This Release: Mitigating Maliciously Tainted and Counterfeit Products through Product Life Cycle

Maliciously Tainted Products can result in: product failure, degraded performance, weakened security mechanisms - allowing malicious functionality to cause critical damage and theft of intellectual property

Counterfeit Products can result in: *For Customers:* loss of productivity, revenue – and critical damage if they fail at critical junctures. *For Providers:* loss of revenue stream and brand damage

To mitigate the risks effectively O-TTPS has process requirements that apply to hardware and software throughout the entire product life



Reference: Types of Supply Chain Threats

<http://ieeexplore.ieee.org/xpl/articleDetails.jsp?arnumber=6717082>

Counterfeit Supply Chain Threats

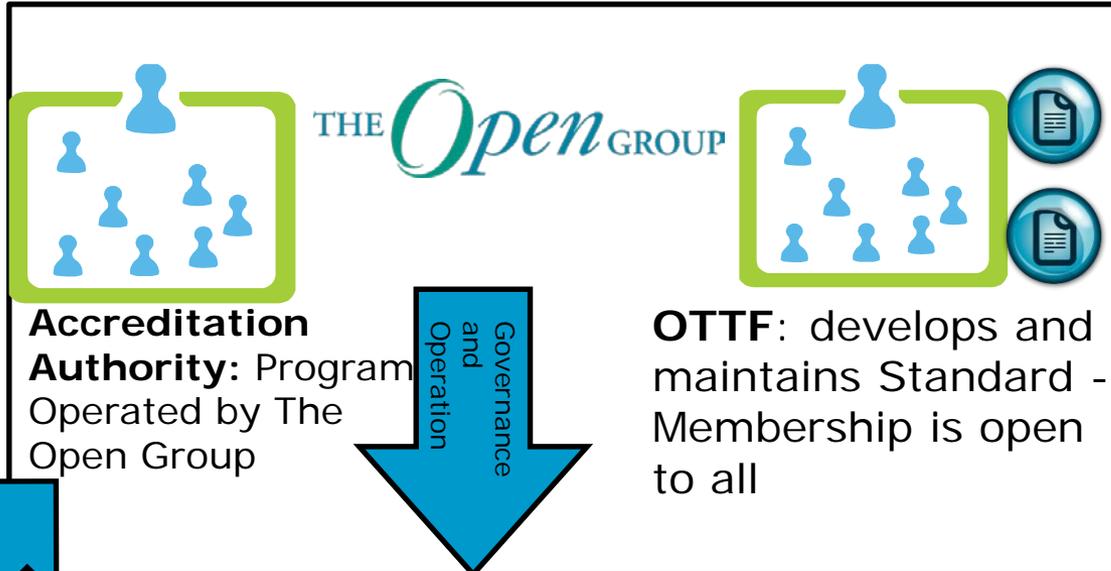
Recycled Counterfeit Components	Components that have been illegally recycled and deceptively presented as new through unauthorized channels.
Second-Run Counterfeit Components	Components, often microelectronic components, that are produced for the OEM but sold through other channels or under assumed names this includes components that do not meet expected quality thresholds of the OEM and are intended for destruction and recycling but instead are sold as authorized components on the open market.
IP Counterfeits	Counterfeit components or products that are manufactured by non-authorized manufactures or dealers that usually entails the theft of IP (intellectual property) in order to manufacture the product or component.
Unauthorized Resale Counterfeit	Sale of products through non-authorized channels or sale of outdated or discontinued products or components. This includes products or components that are withdrawn from the market by the OEM.

Tainted Supply Chain Threats

Negligently Tainted	Products that are manufactured using shoddy development or engineering practices with the intent to deceive customers as to the quality and value. Such products or components are not supported by a timely defect resolution or patch process and are intended to deceive and defraud.
Maliciously Tainted	Products or components that are intended to maliciously harm or exploit the end-user. This includes maliciously designed products or products that contain, by inclusion, a malicious component (e.g., inclusion of a virus during packaging, or a component that has intentionally been designed with malicious intent)
Shared Code Taint	Shared or Open source components that are integrated in a product or solution that are not properly maintained and therefore contain excessive defects and vulnerabilities.
Shared Service Taint	Web-based applications that are compromised by a shared service component that is tainted by the inclusion of one or more of the other categories of tainted threats (Negligent, Malicious, or Shared).

The O-TTPS Accreditation Program

Based on
Warranty from
Organization &
Conformance
Assessment



Open
Trusted
Technology
Providers™

Scope
Flexible.
Whole
organization
to one product



Warrant &
Represent

Application

Engages

O-TTPS Accreditation Program

Vendor neutral program: Accreditation Authority responsible for accreditation of 3rd party assessors, appeals, certificates, logo-use, consistency across accreditations

Success!



Open to all
Component Suppliers,
Providers, Integrators –
*Do Not need to be an
Open Group Member*



Program logo used
to support
accreditation
claims

O-TTPS Recognized 3rd Party Assessors



The Scope of Accreditation

- ❑ Organization chooses their scope: product, product line/business unit, an entire organization.
- ❑ Organization must warrant they are conformant to the O-TTPS requirements throughout the Scope.
- ❑ If the Scope is only one product it will be used to assess conformance to each of the O-TTPS requirements.
- ❑ If the Scope is a product line/business unit or organization then a set of representative selected products will be used to assess conformance throughout the scope.

THE *Open* GROUP O-TTPS Accreditation Program

Home

Registers

- Accreditation Register
- Recognized Assessor Register

Accreditation

- Getting Started
- Accreditation Policy
- Accreditation Requirements
- Accreditation Agreement
- Accreditation TMLA
- Accreditation Fees
- Conformance Statement
- ISCA Document
- Accreditation Package Document

Recognized Assessors

- Getting Started
- Recognized Assessor Agreement
- Recognized Assessor TMLA
- Recognized Assessor Fees
- Assessment Procedures
- Assessor Examination

About O-TTPS

- Frequently Asked Questions
- O-TTPS Standard

Contact Us

- Request Help or Ask a Question
- Contact the Accreditation Authority
- Problem Reporting and Interpretations

O-TTPS Accreditation Register

There are 1 Accredited Organizations

Organization	Scope of Accreditation	Standard	First Accredited	Re-Accreditation	Status	Conformance Statement	Certificate
International Business Machines Corporation	IBM's Application Infrastructure and Middleware (AIM) Software Business Division	Open Trusted Technology Provider™ 1.0	30-Jan-2014	30-Jan-2017	Accredited		



Open Trusted Technology Provider™ 1.0

This is to certify that the following Scope of Accreditation:

**IBM's Application Infrastructure and Middleware (AIM) Software
Business Division**

from

**International Business Machines
Corporation**

is accredited and complies with the requirements in the Open Trusted
Technology Provider™ Standard (O-TTPS) Accreditation Program for:

Open Trusted Technology Provider™ 1.0

Date registered: *30 January 2014*

Valid until: *30 January 2017*

Two Assurance Components: Warranty by the Organization and Assessment by O-TTPS Recognized Assessors

- ❑ **All The Open Group programs include a warranty of conformance from the certified/accredited Organization**
- ❑ **The Organization's warranty helps ensure that within the Scope of Accreditation:**
 - Organizations conform to the O-TTPS requirements
 - Organizations remain conformant throughout the accreditation period
 - If there is a non-conformance, the Organization's practices must come back into conformance in a timely manner
- ❑ **If an Organization doesn't remain conformant:**
 - They can't use the Trademark Logo
 - They are removed from the public register
- ❑ **The Open Group uses trademarks because:**
 - Trademark law can be used to prevent false claims
 - Use of a trademark is controllable

The Open Group - 25 years of Certification Experience

□ Architecture Certifications

- TOGAF® - architecture development method
- Open CA - architecture skills and exp.
- ArchiMate® - arch. modelling language

□ IT Skills Certifications

- Open CITS

□ UNIX®

- Specification, Test suites, certification

□ NASPL (Lotteries & Vendors)

- Standards, certification program development and operation – work with 3rd Party Assessors

□ SIF (Schools Interoperability)

- Certification development and operation on behalf of SIF

O-TTPS: Launched Feb. 3, 2014, FACE: In Development

□ HTNG

- Hotel Management: certification program development and operation

□ Near Field Communication Forum

- NFC certification development and operation - work with 3rd party labs, policy development for test lab recognition & 17024 accreditation

□ Open FAIR

- A leading risk analysis method

□ IEEE POSIX®

- Test tools, certification program development and operation in partnership with IEEE SA

□ LSB

- Test tools for Linux, certification program development and operation – under LSB identity

□ WAP

- Certification operation, initially for WAP Forum, then as a Forum under The Open Group

<http://www.opengroup.org/certifications>

Assessments by 3rd Party Labs

- ❑ **Publically Available Assessment Procedures**
 - Help achieve objectivity, repeatability, and consistency across accreditations
- ❑ **Two types of requirements/evidence to be assessed: process and implementation**
 - Process – Need to provide evidence there are documented processes
 - Implementation – Need to provide evidence that the processes were implemented
- ❑ **Formal Recognition of O-TTPS 3rd party labs**
 - ❑ Must meet established criteria and assessors must pass O-TTPS Assessor exam.
 - ❑ Receive certificates and listed on public registry

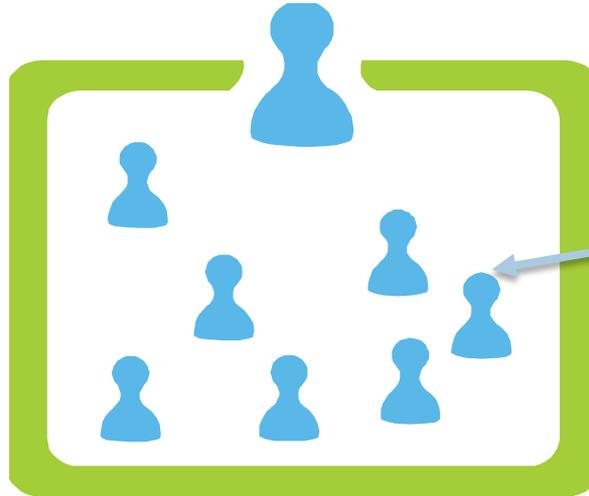
O-TTIPS Recognized Assessor Requirements

Recognized Assessor Company

Operates an **already** certified management system for organizational processes **using industry accepted standards**.

These standards include documentation management, record control, personnel training, resource management, internal auditing and preventive and corrective actions.

Two components



Competent assessors

Have **already** been trained and have a minimum of 2 years' experience in performing process audits or assessment of process conformance to standards based upon review of process documentation and associated records of process implementation.

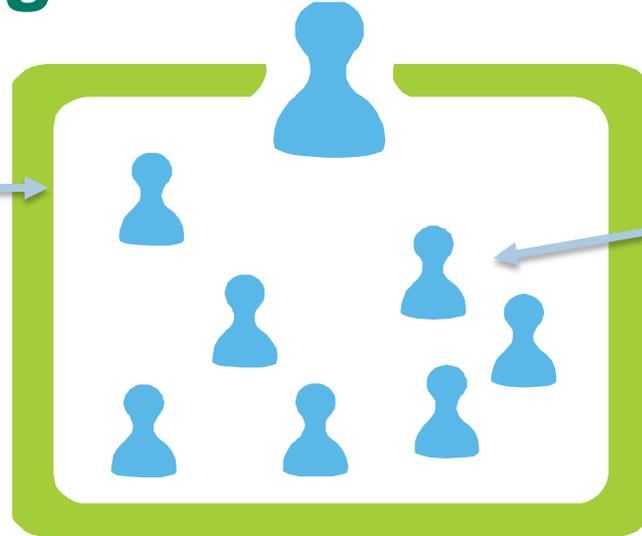
*The Open Group Program relies on **existing** compliance with industry norms using standards commonly specified for information assurance (IA) assessor companies and process assessors*

O-TTPS Recognized Assessor Requirements

Recognized Assessor Company

Accepted standards:

- **ISO/IEC 17020:**
2012: Conformity Assessment – Requirements for the operation of various types of bodies performing inspection,
- **ISO/IEC 17021:2011:**
Conformity Assessment – Requirements for bodies providing audit and certification of management systems,
- **ISO/IEC 17025:2005:**
General requirements for the competence of testing and calibration laboratories



Competent assessors

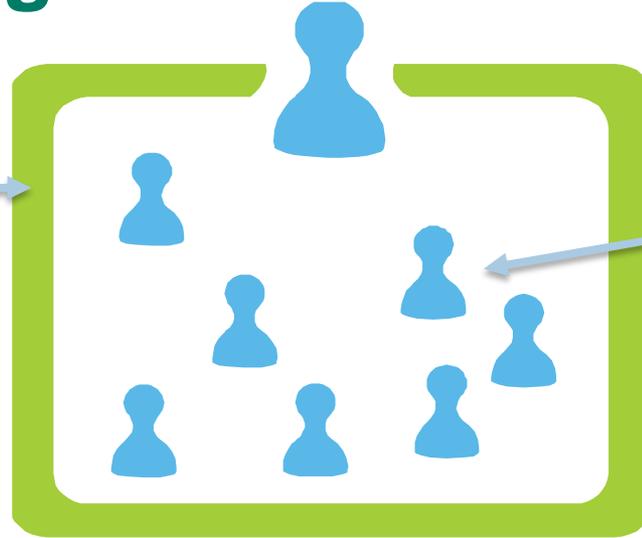
Accepted qualifications:

- **Lead auditor**
 - ISO/IEC 27001
 - ISO 9001
- **CMMI-DEV appraisers**
- **ISO/IEC 15408 or Common Criteria evaluator** (with experience in evaluating life-cycle assurance requirements)
- **ISO/IEC 19790 or FIPS 140-2 tester** with experience in testing the process requirements of that standard

*The Open Group Program relies on **existing** compliance with industry norms using standards commonly specified for information assurance (IA) assessor companies and process assessors*

O-TTPS Recognized Assessor Requirements

Recognized Assessor Company



Has established a **process for performing O-TTPS accreditations** in accordance with its own established management system requirements and The Open Group Assessment Procedures

*The Open Group Program **builds on existing standards** assuring that Subject Matter Expertise is established in the assessor companies*

Competent assessors

Have sufficient skills in:

- Supply chain management terminology and techniques
- Technical knowledge of O-TTPS Attributes & the assessment program
- Have successfully completed the **O-TTPS Assessor Exam**

O-TTPS Accreditation: Summary

- ❑ The Organization can be a component supplier, a provider, or integrator
- ❑ The Organization warrants and represents their conformance to requirements throughout their declared Scope of Accreditation
- ❑ Scope up to Organization: product, product-line, organization
- ❑ Warranty backed by evidence of conformance and assessment of evidence by 3rd party O-TTPS Recognized Assessors
- ❑ The Open Group operates vendor-neutral program, provide oversight and consistency across applications
- ❑ Successful applicant gets certificate and use of trademark and logo
- ❑ The Open Group manages trademark and logo use, problem reporting and appeals process.
- ❑ The accreditation period is 3 years before required renewal
- ❑ O-TTPS accreditation open to any organization
 - don't need to be a member
- ❑ O-TTPS Recognized Assessor Program, managed by The Open Group

Resources

- ❑ [The Open Group Trusted Technology Forum](#)
- ❑ [The O-TTPS \(Standard\) Version 1.0](#)
- ❑ [The Open Group represents OTTF at Congress](#)
- ❑ [O-TTPF Vendor Testimonials](#)
- ❑ [The O-TTPS Accreditation Policy Version 1.0](#)
- ❑ [OTTF Podcast \(Dana Gander with: Brickman, Lipner, Lounsbury, and Szakal\)](#)
- ❑ [Press Release Feb 3, 2014 – Launch of the O-TTPS Accreditation Program](#)
- ❑ [The Open Group](#)

Thank You!

**For more information on
the O-TTPS Accreditation Program visit
<http://www.opengroup.org/accreditation/o-ttps>**

**For more information on the Forum visit:
<http://www.opengroup.org/subjectareas/trusted-technology>**

**For more information on Membership contact
[Mike Hickey at m.hickey@opengroup.org](mailto:m.hickey@opengroup.org)**