Supply Chain Security for COTS Products:

The Bigger Picture.

Fiona Pattinson

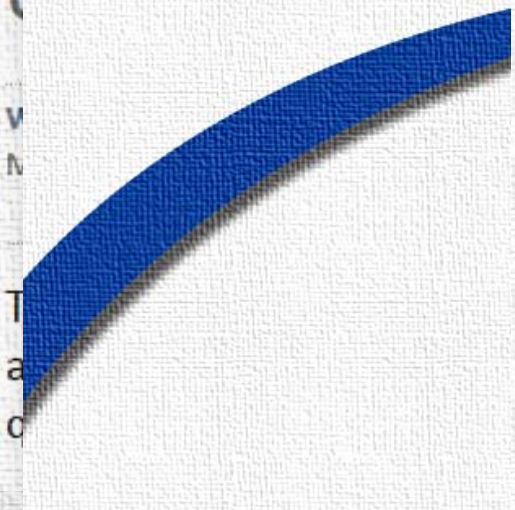
Andras Szakal

A SPECIAL REPO

Counterfeit

Increasing Awaren
Developing Counte

March 2011



NATIONAL STRATEGY FOR GLOBAL SUPPLY CHAIN SECURITY

JANUARY 2012

Types of Supply Chain Threats

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Unauthorized Resale Counterfeit	Sale of products through non-authorized channels or sale of outdated or discontinued products or components. This includes products or components that are withdrawn from the market by the OEM.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 Open Group Membership

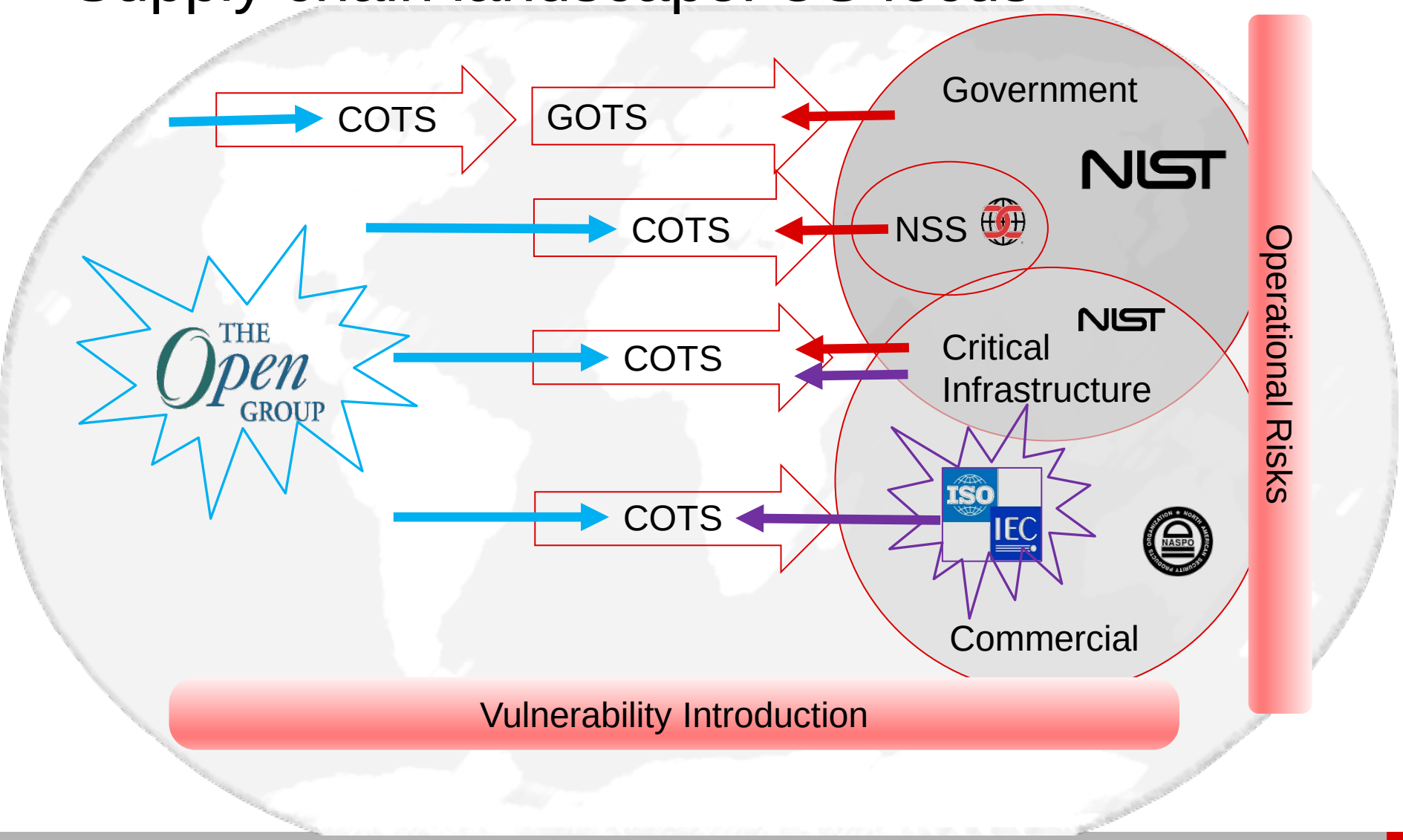
THE Open GROUP

The Open Group CyberSecurity Activities

Infosec Thought Leadership	Security Forum	Real Time & Embedded Systems	Trusted Technology Forum
Open Standards & Best Practices	Open Standards & Best Practices	Open Standards	Supply Chain Security Standards, Best Practices
• De-perimeterization • Identity management • Data protection • Cloud security	• Security architecture • Information security management • Risk management standards, best practices, and certification • Compliance & security automation	• MILS • Software assurance • High assurance certification • Dependability	• Open Trusted Technology Provider Standard • Addressing maliciously tainted and counterfeit products • Accreditation Program

THE Open GROUP

Supply chain landscape: US focus



THE Open GROUP

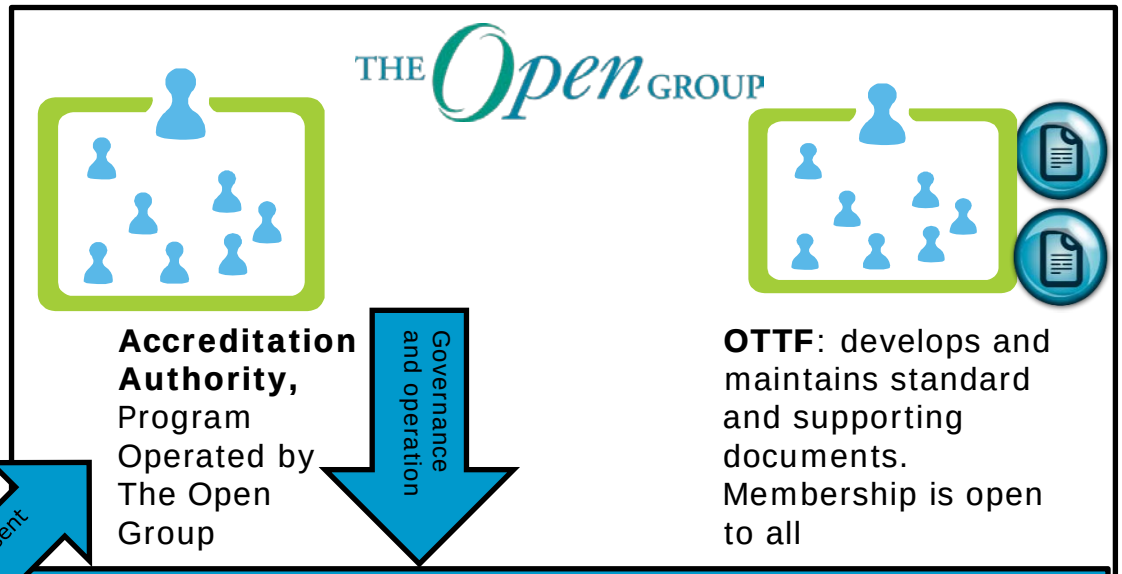
The Open Group – O-TTPS V1

Status	Published: Available free from http://www.opengroup.org/bookstore/catalog/c139.htm
Accreditation	Yes: (In trial): Public program due early 2014
Focus	COTS developers (providers) and their upstream suppliers. An open international standard containing a set of organizational guidelines, requirements, and recommendations for integrators, providers and component suppliers to enhance the security of the global supply chain and the integrity of Commercial Off The Shelf (COTS) Information and Communication Technology (ICT).
Assurance consumers	Downstream organizations; Government procurers, integrators, users
Threats	Maliciously tainted products Counterfeit products

O-TTPS: Proposed Accreditation Program

Status:

Pilots underway now.
Public launch: November 2013



Scope Flexible – Defined by Applicant Whole organization to one product

Warrant & Represent

Application

Engages

Verifies compliance

Success!

Applicants (Component Supplier, Provider, Integrator)

Trusted Providers

3rd Party Assessors

Program logo used to support accreditation claims

THE Open GROUP

NISTIR 7622

Notional Supply Chain Risk Management Practices for Federal Information Systems

Jon Boyens
Celia Paulsen
Nadya Bartol
Rama Moorthy
Stephanie Shankles

http://dx.doi.org/10.6028/NIST.IR.7622

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

NIST Special Publication 800-161

Initial Public Draft

Supply Chain Risk Management Practices for Federal Information Systems and Organizations

Jon Boyens
Celia Paulsen
Computer Security Division
Information Technology Laboratory

NIST: NIST-IR 7622 : NIST SP 800-161

Status	NIST-IR Published: Available free from http://csrc.nist.gov/publications/ NIST SP 800-161 Draft: Public comment
Accreditation	No: Although this may become part of the C&A associated with the FISMA program: The draft is intended to be supplemental to SP 800-53 (Note that O-TTPS is referenced in the draft for COTS products)
Focus	Guidance to federal departments and agencies on identifying, assessing, and mitigating ICT supply chain risks at all levels in their organizations
Assurance consumers	Downstream organizations; Government procurers, integrators, users
Threats	Flexible, identified and managed through supply chain risk assessments : Some examples included

ISO IEC

ISO/IEC JTC 1/SC 27 N12105

ISO/IEC JTC 1/SC 27/WG 4 N412105

REPLACES: N11993

ISO/IEC JTC 1/SC 27

Information technology - Security techniques

Secretariat: DIN, Germany

DOC TYPE:	text for DIS ballot
TITLE:	**Text for ISO/IEC DIS 27036-1:2013-01-17(E) -- Information technology — Security techniques — Information security for supplier relationships — Part 1: Overview and concepts**
SOURCE:	**ITTF**
DATE :	2013-01-17
PROJECT:	1.27.73.01 (27036-1)
STATUS:	**This document is currently undergoing a 3-month DIS letter ballot at the JTC 1 level.** **The P-members of JTC 1 and SC 27 are kindly requested to submit their votes on ISO/IEC DIS 27036-1:2013-01-17(E) directly to the ISO Central Secretariat via the ISO e-balloting application by 2013-04-17.**

	ISO: ISO/IEC 27036 *– Part 1: Overview and concepts* *– Part 2: Requirements* *– Part 3: Guidelines for Information and Communication Technology (ICT) supply chain security*
Status	Final drafts (Parts 1,2,3)
Accreditation	No (Note this may be possible later through ISO certification programs or other certification programs)
Focus	*Supplier and acquirer relationships* Specifies fundamental information security requirements for defining, implementing, operating, monitoring, reviewing, maintaining and improving **supplier and acquirer relationships**;
Assurance consumers	Downstream organizations (integrators and operational users)
Threats	Flexible (Risk identification and management approach)
Notes:	The Open Group standard, OTTPS, is expected to become a part of this standard.

DRAFT

Supply Chain Security Assurance

A Common Criteria Supporting Document (Non-mandatory Guidance type)

Last updated: August 22, 2013

The information and communications technology (ICT) supply chain is a critical global asset which is essential to the global economy and security. Maintaining an ICT product's integrity through this complex global supply chain requires increased security focus. As a result, providers of commercial software and hardware products are using techniques to mitigate vulnerabilities introduced via this supply chain.

Common Criteria	**Common Criteria: Supply Chain Technical Working Group** **Common Criteria Supporting Document**
Status	Draft
Accreditation	Not currently Once accepted optional use during evaluation of IT products under CC
Focus	CC evaluated products
Assurance consumers	Downstream organizations; Government procurers, integrators, users
Threats	Maliciously tainted products Counterfeit products
Notes:	Will be applicable to the subset of CC evaluated products only. High assurance evaluations , destined for commercial space and for some governments, should find this a useful augmentation for product assurance

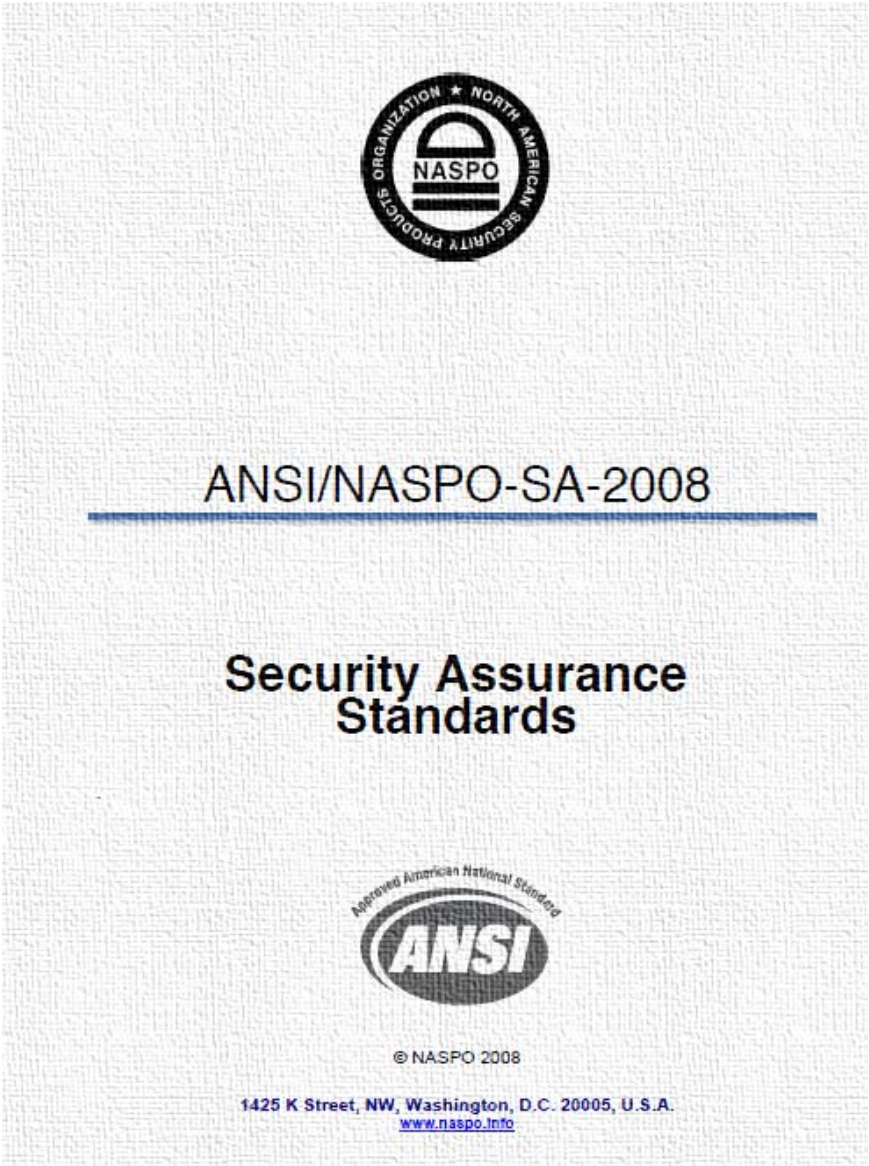
An example of many specialised standards in the supply chain space.

This one is used mainly in the US for assuring counterfeit and taint threats to high-value assets have been addressed according to the NASPO SA-2008 standard.

Focused on security documents / Pharmaceutical industry.

Works in ISO on ISO/TC 247 Fraud countermeasures and controls

http://www.naspo.info/certification



Summary

- We have aimed to show how many of the standards and supply chain initiatives fit together to provide a coordinated response.
- Collaboration with a variety of industry and government bodies is key to success.
  - E.g. Mapping an existing CC certified product to the O-TTPS requirements allowing for potential reuse/recognition.
  - Active collaboration is ongoing. Including:
    - Liaison with Open Group & CCDB being established
    - SC TC working on Supply Chain package
    - Liaison between CCDB and ISO
    - Liaison between the Open Group and ISO
- We also benefit from a small expert community with much overlap between organizations

Questions?

Securing the Global Supply Chain

Enabling Providers to Raise the Bar on Security and Integrity

The Open Group Trusted Technology Forum™ (OTTF)

"Build with Integrity

Buy with Confidence™

July, 2013

THE Open GROUP

Meeting Objectives

- **Meeting Objectives from the OTTF perspective:**
  - Raise awareness, in relation to The Executive Order, of the OTTF as a global consortia and an effective industry-government partnership in addressing major relevant cybersecurity threats:
    - tainted products that enable security vulnerabilities
    - counterfeit products that can be faulty and tainted
  - Obtain guidance on how best to work cooperatively with the Administration's stated interest in:
    - Public/private partnerships related to cybersecurity and supply chain
    - Leveraging existing industry efforts that are practical and scalable
  - Seek input on next steps for broadening exposure and increasing adoption for the OTTF within the US government

The Open Group Membership

THE Open GROUP

What Does The Open Group Do?

- **Membership & Events**
  - Forums & Work Groups: Architecture, Security, Real-Time and Embedded Systems, Cloud, SOA, OTTF etc.
  - International & Regional Conferences

- **Standards and Certification - Over 25 years experience**
  Voluntary consensus standards and certification programs through The Open Group Standards Process consistent with OMB Circular A-119
  - **People & Organizations:** TOGAF®, Architects, IT Specialists, Lotteries (Quality Assurance Best Practices), O-TTPS™
  - **Products & Technology:** NFC Forum, UNIX®, WAP, Architecture Tools
  - **Defense Standards:** DirecNet, FACE™

THE Open GROUP

The Open Group CyberSecurity Activities

Infosec Thought Leadership	Security Forum	Real Time & Embedded Systems	Trusted Technology Forum
Open Standards & Best Practices	Open Standards & Best Practices	Open Standards	Supply Chain Security Standards, Best Practices
• De-perimeterization • Identity management • Data protection • Cloud security	• Security architecture • Information security management • Risk management standards, best practices, and certification • Compliance & security automation	• MILS • Software assurance • High assurance certification • Dependability	• Open Trusted Technology Provider Standard • Addressing maliciously tainted and counterfeit products • Accreditation Program

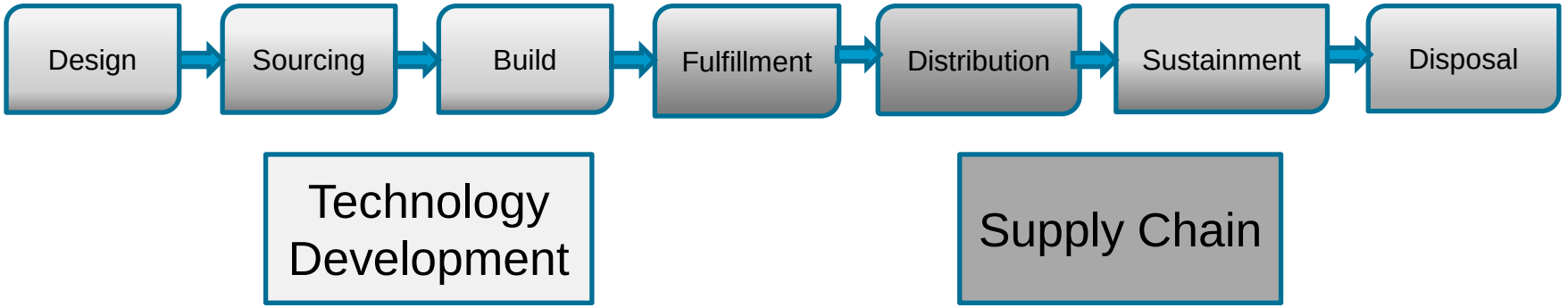
THE Open GROUP

OTTF Background

- **Government-industry roundtable discussion in 2009**
  - Initiated by DOD/AT&L, 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

O-TTPS: Mitigating Maliciously Tainted and Counterfeit Products

- The Open Trusted Technology Provider Standard (O-TTPS) **released in April, 2013** – 50 page document on requirements for organizational best practices
- **The result of over 3 years of collaborative consensus-based effort**
- Apply across product life cycle. Some highly correlated to threats of **maliciously tainted and counterfeit products** - others more foundational but considered essential



- **2 areas of requirement**s – often overlap depending on product and provider:
  - Technology Development - *mostly* under the provider's in-house supervision
  - Supply Chain activities *mostly* where provider interacts with third parties who contribute their piece in the product's life cycle

THE Open GROUP

O-TTPS: Technology Development

- Product Development/Engineering Requirements in:
  - Software/Firmware/Hardware Design Process
  - Development/Engineering Process and Practices
  - Configuration Management
  - Quality/Test Management
  - Product Sustainment Management
- Secure Development/Engineering Requirements in:
  - Threat Analysis and Mitigation
  - Run-time Protection Techniques
  - Vulnerability Analysis and Response
  - Product Patching and Remediation
  - Secure Engineering Practices
  - Monitor and assess the impact of changes in the threat landscape

O-TTPS: Supply Chain Activities

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

OTTF Principles

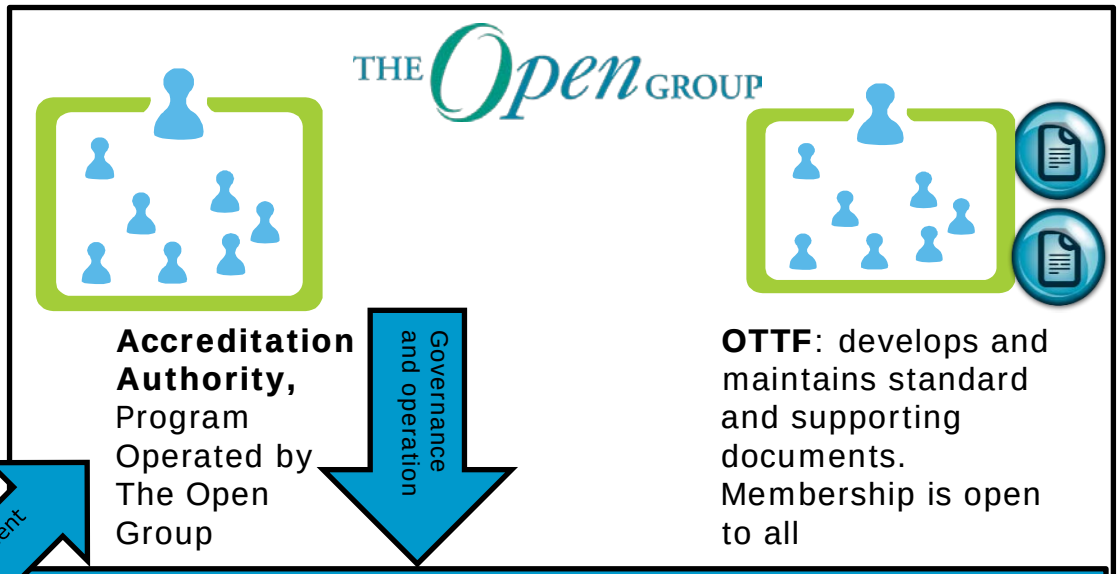
The OTTF is developing their standards and accreditation programs according to these principles:

- ***Practical and effective*** **-** Practitioner based, evidence that it works in the field
- ***Reasonable*** **-** Achievable and implementable by a wide variety of vendors and stakeholders
- ***Affordable*** **-** Reasonably cost effective to implement
- ***Open*** **-** Based on open standards and recognized industry best practices – publically available to all
- ***Organizational/Process Based Accreditation*** **-** Flexible enough that an organization can choose their own scope of accreditation (product, product-line, entire organization)

O-TTPS: Proposed Accreditation Program

Status:

Pilots underway now.
Public launch: November 2013



Scope Flexible – Defined by Applicant Whole organization to one product

Warrant & Represent

Application

Engages

Verifies compliance

Success!

Applicants (Component Supplier, Provider, Integrator)

Trusted Providers

3rd Party Assessors

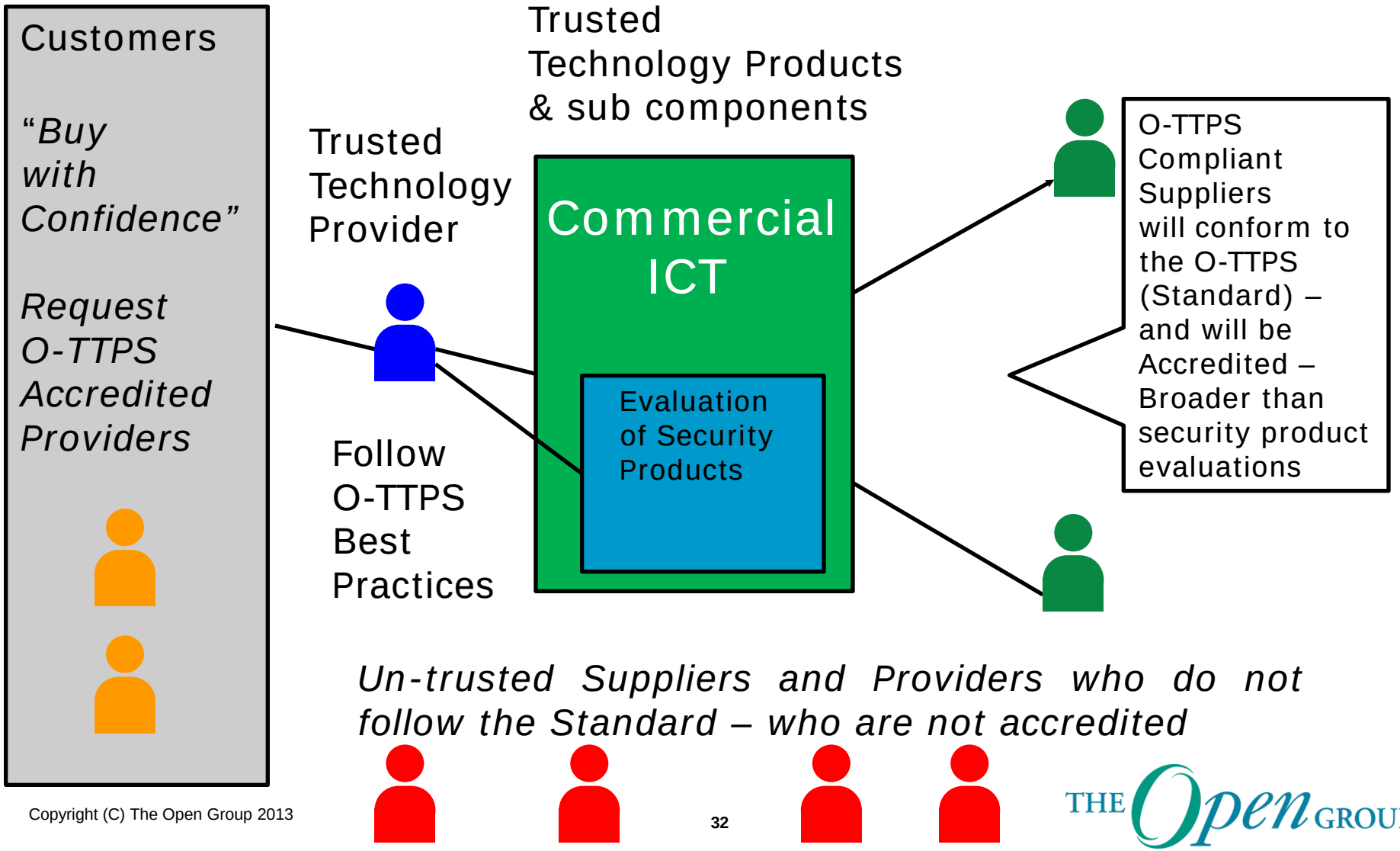
Program logo used to support accreditation claims

THE Open GROUP

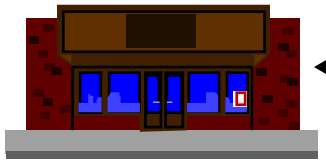
O-TTPS: Planned Accreditation Program

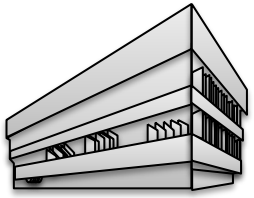
- The Applicant can be a Component Supplier, a Provider, or an Integrator
- The Applicant warrants and represents their conformance to requirements throughout their declared Scope of Accreditation – that is they claim that they follow the best practices through out the product life-cycle, including supply chain cycles for all of the products in their declared Scope
- Scope up to Applicant: product, product(s), product-line, organization, etc.
- Warranty backed by evidence of conformance and assessment of evidence by 3rd Party Assessors
- The Open Group will operate 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
- Pilot Accreditations Underway now
- Planned launch of a public O-TTPS accreditation program – open to any organization – don't need to be a member – planned for November 2013

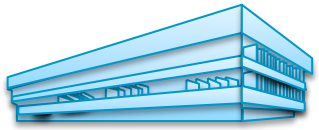
Objective: Customers Buy with More Confidence:
Providers & Suppliers Can Extend Supply Chain Security



THE Open GROUP







Customer/Acquirer

Demands Accreditation certificate as evidence of conformance to Open Trusted Technology Provider™ standards

Integrator

Will seek business partners who can meet Open Trusted Technology Provider™ requirements

Standards Body

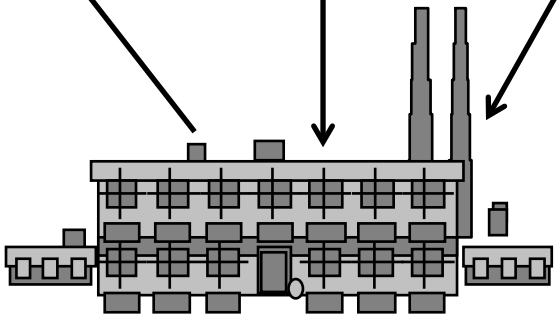
Will seek ways of achieving market up-take/ integrity of standards

Business Partners

Standards Process

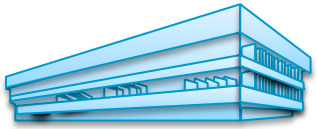
Alliance

Business Partners



Accreditation

Process



Component Suppliers

May be hardware, software, global, open source - or not - multiple supplier layers

Provider

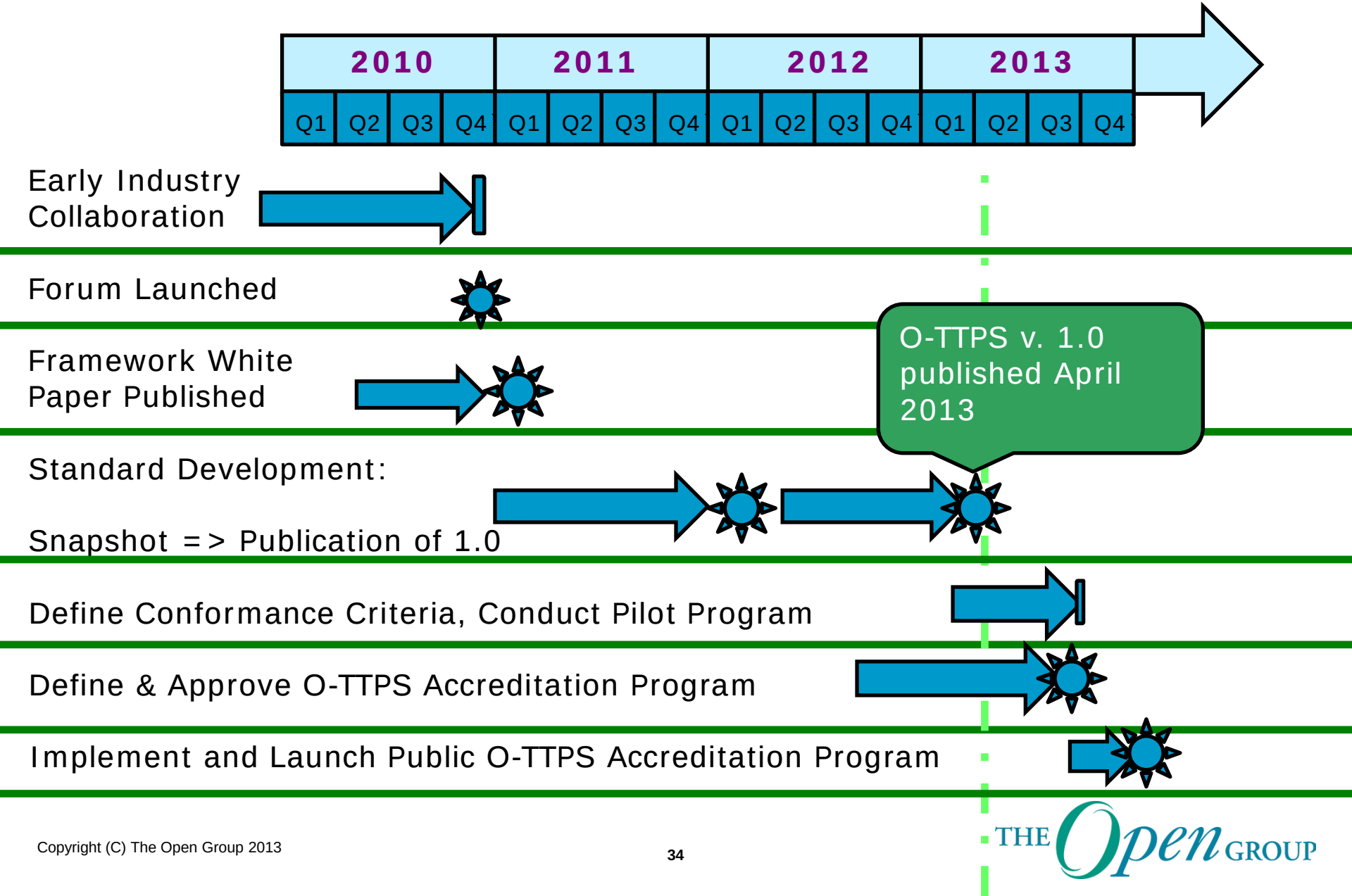
Will seek business partners who can meet Open Trusted Technology Provider™ requirements

Accreditation/ Accreditation Body

Must be independent & vendor/technology-neutral

THE Open GROUP

OTTF Milestones and Time Frames



THE Open GROUP

Market Impact and Outreach

- **GAO Report on Supply Chain, published in May 2013**
  - Identified O-TTPS as one of "the two industry-led efforts most frequently discussed during [their] interviews."
- **NASA SEWP V Draft RFP issued in March 2013**
  - Supply Chain recommendations include that providers, resellers utilize O-TTPS standard and accreditation
- **The Open Group represents OTTF at Congress – March 2012**
  - Sub-committee hearing on Supply Chain (Mitchell Komaroff testified at same hearing for DOD)
- **Early days: briefed & obtained feedback on O-TTPS Draft Standard**
  - NSA and NIAP
  - CESG in UK
  - US Senate and US House staff, US Department of Commerce
- **Met with government agencies in: Japan, UK, India, China**
- **The Open Group extends International Outreach with:**
  - **Taiwan, Brazil, Dubai, Australia, France, Sweden, Spain, UK**

THE Open GROUP

Standards Harmonization

- **NIST**
  - Participating in the NIST CyberSecurity Framework Workshops
- **ISO**
  - The Open Group is recognized PAS (Publicly Available Specification) submitter
    - Allows The Open Group to submit their standards to ISO
    - Exploring PAS submission of O-TTPS to ISO
  - Liaisons with:
    - Work Group 3, Security Evaluation Criteria, produces standards related to Common Criteria
    - Work Group 4, Security Controls and Services, producing ISO/IEC 27036 on Information Security for Supplier Relations.
- **Common Criteria**
  - Working with CCDB to create an OTTF Liaison with and harmonize our work in supply chain.

O-TTPS - Ready to Solve the Problem

- **The O-TTPS (Standard) is:**
  - **Freely available today**
    - Everyone can download and begin preparing for accreditation
  - **Anyone can join the OTTF**
    - to help define, evolve, maintain the standard and accreditation program
- **The O-TTPS Accreditation Program is:**
  - **In Pilot now, Public Launch at end of 2013**
  - **Likely the first global assessment program consistently measuring evidence of product-related best practices for**:
    - basic hygiene in product development and secure engineering
    - supply chain security
  - **Accreditation available to all**
    - component suppliers, providers, and integrators around the world
    - Membership in the OTTF is not required for accreditation

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
- OTTF Podcast (Dana Gander with: Brickman, Lipner, Lounsbury, and Szakal)
- The Open Group

Thank You!

O-TTPS (Standard) – Free to download at:

https://www2.opengroup.org/ogsys/catalog/c139

For more information about the OTTF contact:

Sally Long, The OTTF Forum Director
s.long@opengroup.org

THE Open GROUP