

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”™*



Who is The Open Group?

- ❑ The Open Group is an international vendor- and technology-neutral consortium - that organizations rely on to:
 - Lead the development of IT standards and certifications
 - Enable access to key industry peers, customers and suppliers
 - Provide guidance and an open environment to ensure vendor-neutrality
- ❑ The Open Group includes:
 - more than 20,000 individuals
 - representing more than 400 member enterprises
 - from all sectors of the industry in more than 80 countries.
- ❑ The Open Group has offices in:
 - Reading in UK, San Francisco and Boston in US, Sao Paulo in Brazil, and in Japan, China, South Africa, France, UAE, Sweden, and Turkey.

What Does The Open Group Do?

❑ Membership & Events

- Forums (Architecture, Security, Real-Time and Embedded Systems, OTTF etc.) and Work Groups (Cloud, SOA, etc.)
- International Conferences
- Regional Conferences

❑ Standards and Certification

- People – OPEN CA, OPEN CITS, TOGAF™
- Products – UNIX®, WAP, Architecture Tools
- Services - Training

❑ Consortia Services

- Various management services our own managed consortia and to other special interest groups
- OTTF transitioned to an Open Group Forum

OTTF Background

- Roundtable discussion in Q4 of 2009
- Governments and commercial enterprises moving away from high assurance customized solutions – toward Commercial Off The Shelf (COTS) Information and Communication Technology (ICT)
- So want to know how to identify a good COTS ICT product
 - If vendors are making quality products – and in most cases secure and trusted products...
 - Then doesn't it make sense to get together and:
 - establish best of breed best practices for industry
 - *consider a brand that would identify products or providers who implement the best practices*

Getting Together to Define Good/Trusted Products/Providers => OTTF

□ “Trustworthy Commercial Product”

- What’s in it (source code and origin/pedigree)
- Who built it (development and manufacturing)
- How will it be sustained from an OEM perspective
- What were the management, process and quality controls applied
- What are the meaningful supply chain considerations
- What variability and volatility of sub-processes and supply should be expected (opportunistic component sourcing and contract fabrication)
- What other “measures of goodness” can be used or leveraged
- Not a substitute for ISO, NIST, ITU, or CC; Interoperability or protocol level compliance or certification

What are
Industry's
Expectations

These are some of
Government(s)'
Expectations

Open Group Trusted Technology Forum

SL2

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™*”

IBM

CISCO

ORACLE

Kingdee
金蝶, 企业管理专家

Microsoft®



EMC²
where information lives®

ca
technologies

MOTOROLA SOLUTIONS

Fraunhofer
SIT

APEXASSURANCE
GROUP



JUNIPER
NETWORKS

Raytheon



BOEING

ASEC
the information security provider

MITRE

SAIC
From Science to Solutions

Booz | Allen | Hamilton

Office of the Under Secretary of Defense for
Acquisition, Technology and Logistics

IDA

TATA
CONSULTANCY SERV

EWA
Enabling a More Secure Future

HUAWEI

Software Engineering Institute | Carnegie Mellon

LOCKHEED MARTIN



THE Open GROUP

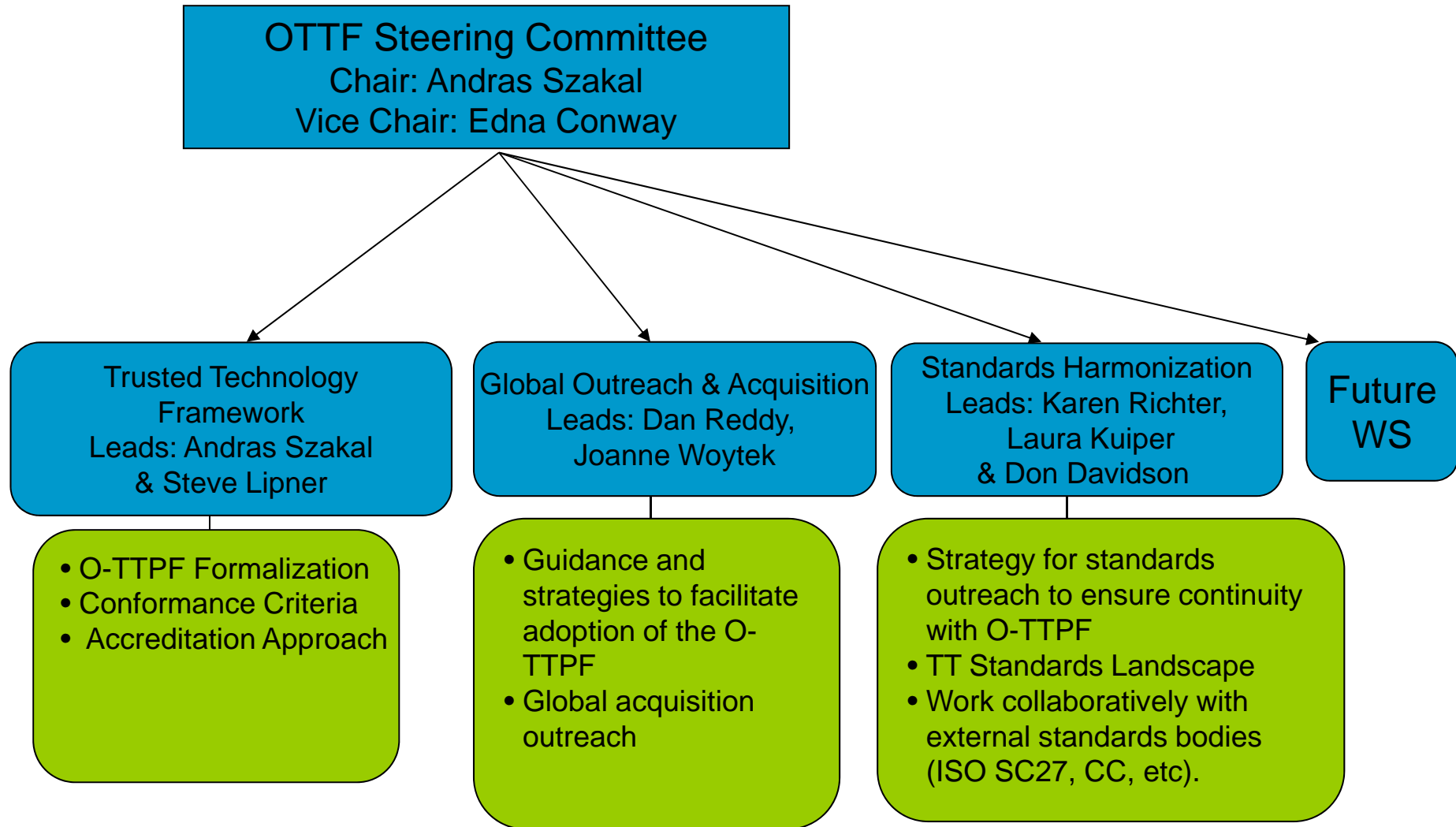
Slide 6

SL2

add BAH

Sally Long, 12/03/2012

OTTF Governing Structure



The OTTF Launched as an Open Group Forum in Dec 2010

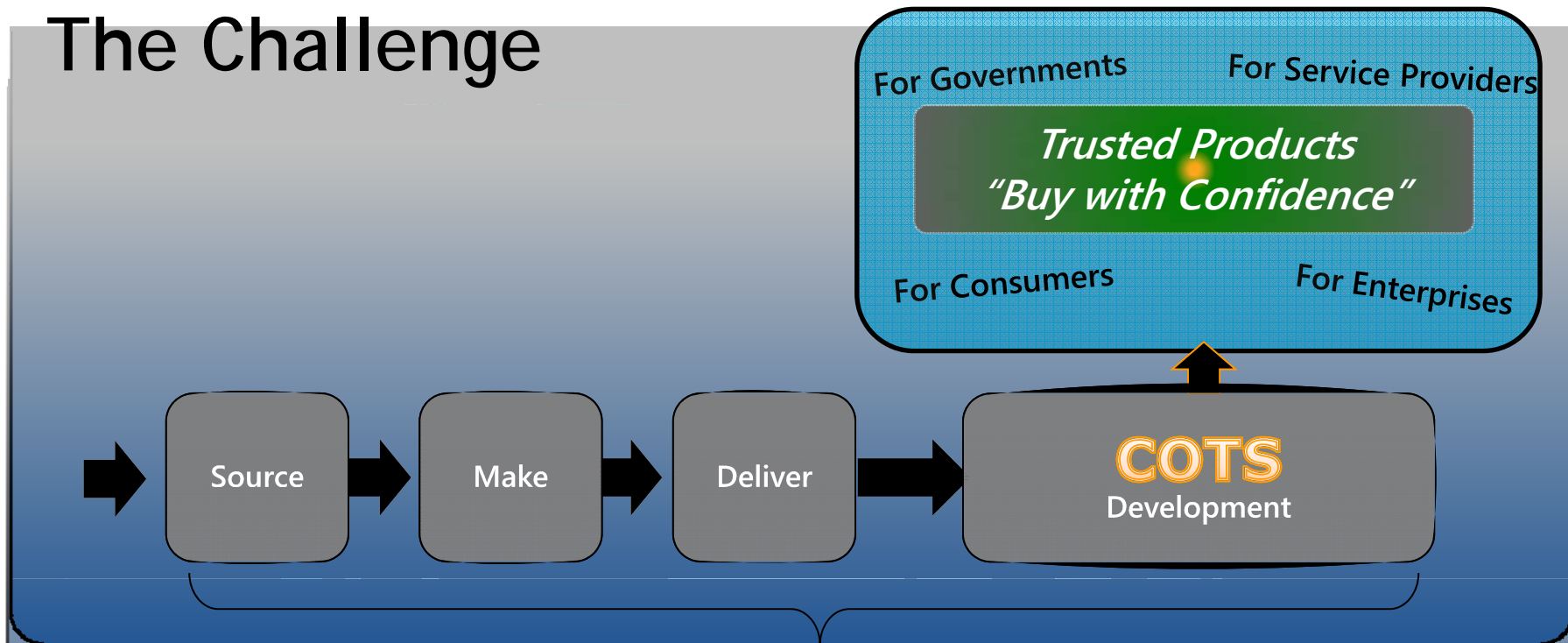
- ❑ Published a Framework White Paper in Feb. 2011
- ❑ Continued to identify best of breed best practices used by industry to enhance security and integrity in COTS ICT Products
- ❑ ***Published The Open Trusted Technology Provider Standard (O-TTPS) Snapshot – Released, March 9, 2012 – codifies best practices across the entire product lifecycle – including the Supply Chain***
- ❑ Evaluating how to use the O-TTPS (Standard) through harmonized accreditation programs
- ❑ Aligning with other standards organizations, certification bodies and regulatory programs
- ❑ Conducting outreach for global recognition and adoption with constituents worldwide

The Challenge – Reflected in OTTF

Memorable Quotes

- ❑ *“Supply Chain is the new black.”*
- ❑ *“I sleep with my husband every night and I trust him but he still may stab me!”*
- ❑ *“Only God created something from nothing - every other business in the world has some kind of supply chain.”*

The Challenge



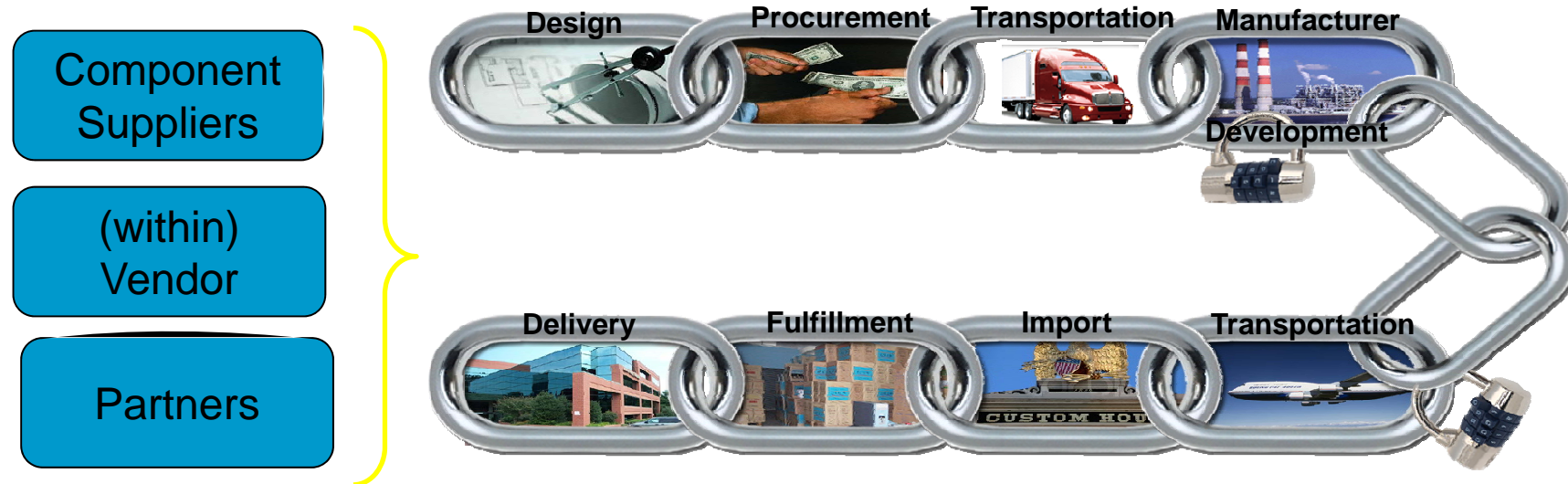
"Build with Integrity"

- ❑ Commercial Off-the-Shelf (COTS) Information and Communication Technology (ICT) leverage a Global Supply Chain
- ❑ Requirement to target security-specific, enumerated supply chain risks, not all risks associated with having a supply chain

***No one approach addresses it all;
We can only succeed together***

Protecting the Technology Supply Chain

Risks – Focusing on Tainted and Counterfeit Products



...pose a threat to the end-to-end product manufacturing / development process

Slide 11

SL5















SHOULD BE add taint and cou terfeit

Sally Long, 12/03/2012

O-TTPS Snapshot – Mitigating Risks for Tainted and Counterfeit Products

- ❑ A tainted product is “produced by the provider and is acquired through reputable channels but has been tampered with maliciously”. - Could result in:
 - product failure, degraded performance, weakened security mechanisms allowing rogue functionality and potentially critical damage
- ❑ A counterfeit product is “produced other than by or for the provider, or is supplied by other than a reputable channel, and is represented as legitimate”. – Could result in:
 - For customers: if product fails at critical juncture – loss of productivity, revenue
 - For providers: loss of revenue stream and brand damage

Technology Supply Chain Threat Matrix

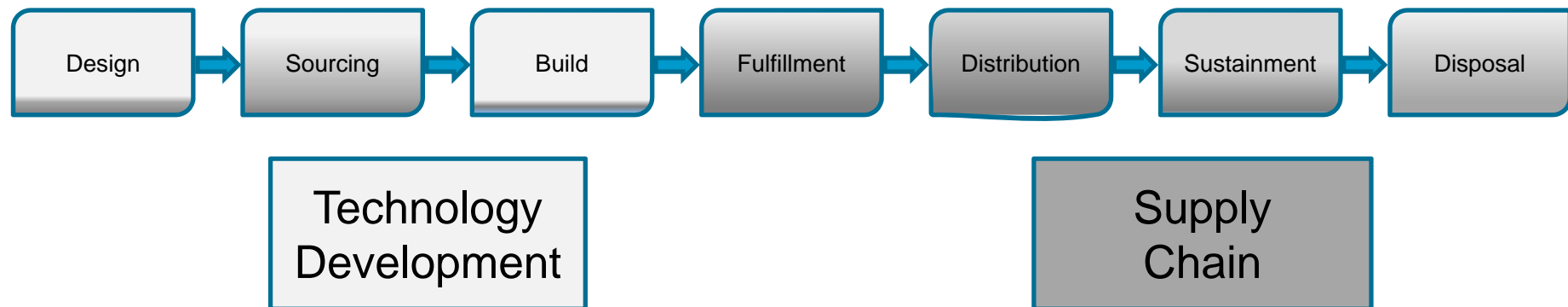
	Taint			Counterfeit		
	Upstream	Provider	Downstream	Upstream	Provider	Downstream
Malware						
Malicious code (masquerading as vulnerabilities)						
Unauthorized “Parts”						
Unauthorized Configuration						
Scrap/ Substandard Parts						
Unauthorized Production						

The OTTF Response to the Challenge

- The OTTF currently plans to:
 - Stage the standard over time – each stage addressing a set of threat models that map to market needs
 - Limit the scope of the Standard to what will become the first version of the standard:
 - COTS ICT Products/Providers
 - First version - best practices that help assure against counterfeit and tainted COTS ICT products
 - Develop a base set of objective and attainable conformance criteria
 - Conduct an internal "conformance pilot" to get some practical experience and then to look at defining a full accreditation program

O-TTPS Snapshot

- ❑ The Standard/Snapshot – released March 9, 2012 – a set of prescriptive requirements and recommendations for organizational best practices
- ❑ Apply across product life cycle. Some highly correlated to threats of taint and counterfeit - others more foundational but considered essential.



- ❑ 2 areas of requirements – that 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

O-TTPS:

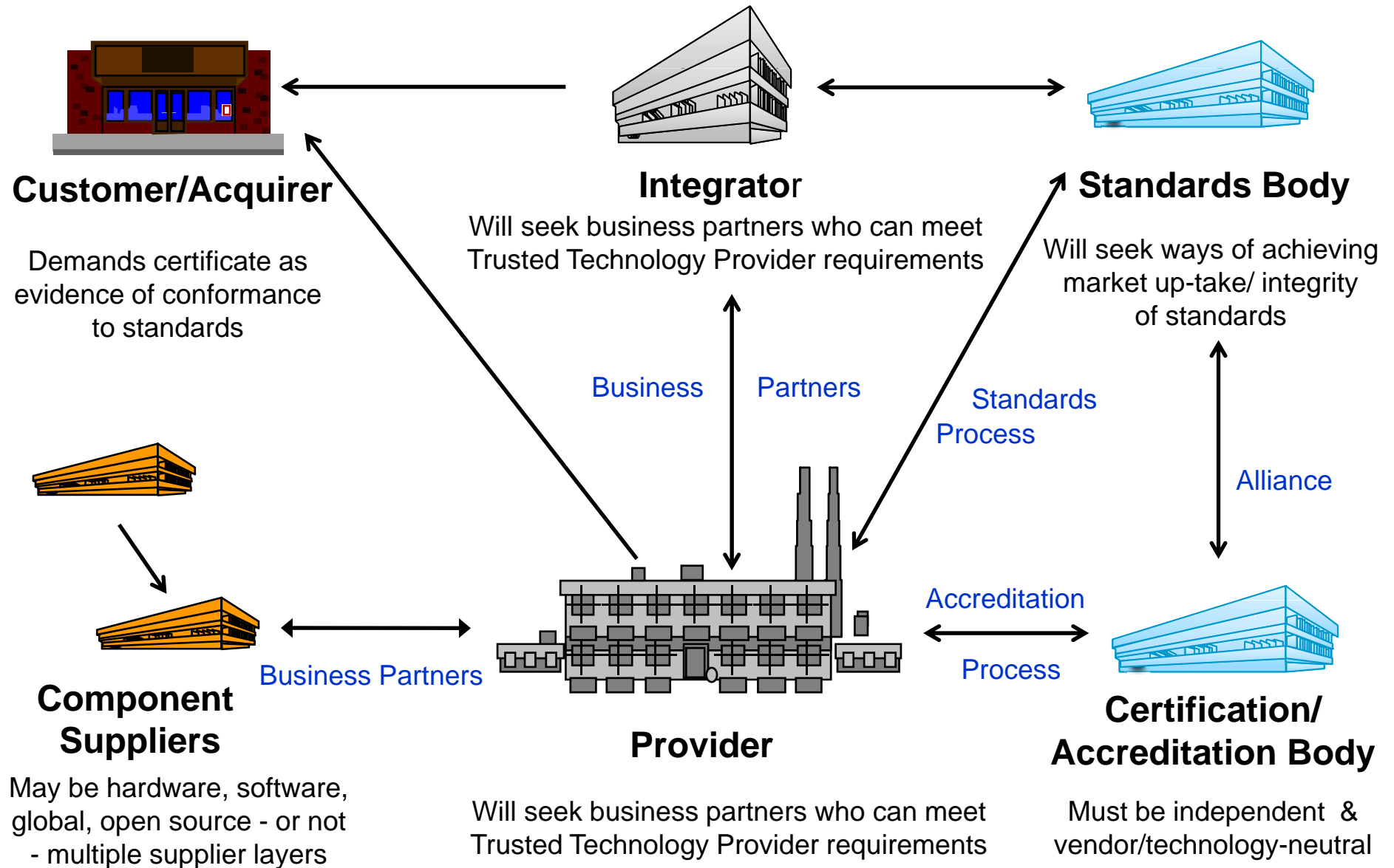
Technology Development Activities

- ❑ 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:

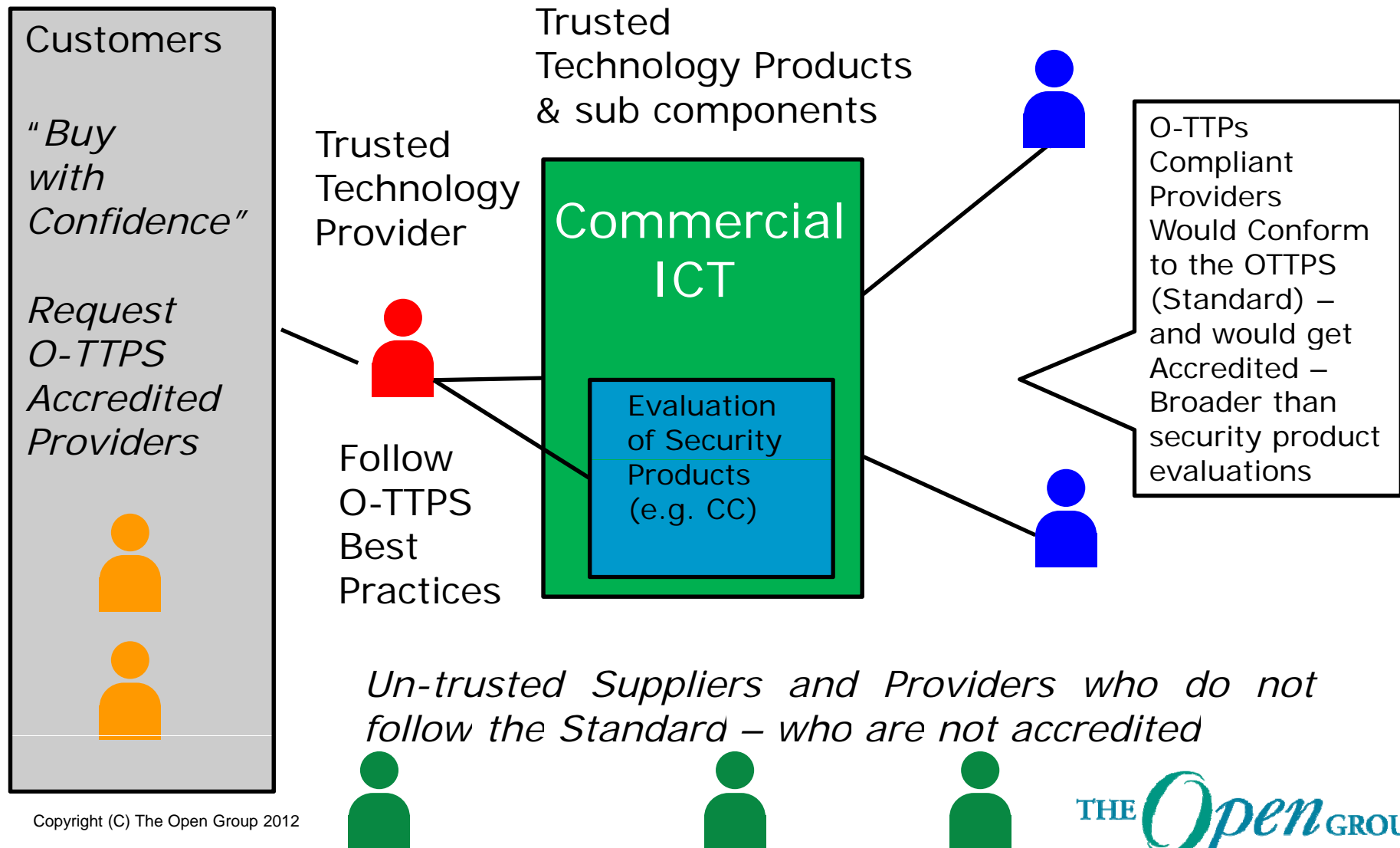
- Risk Management
- Physical Security
- Access Controls
- Employee and Supplier Security
- Business Partner Security
- Supply Chain Security Training
- Information Systems Security
- Trusted Technology Components
- Secure Transmission and Handling
- Open Source Handling
- Counterfeit Mitigation
- Malware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



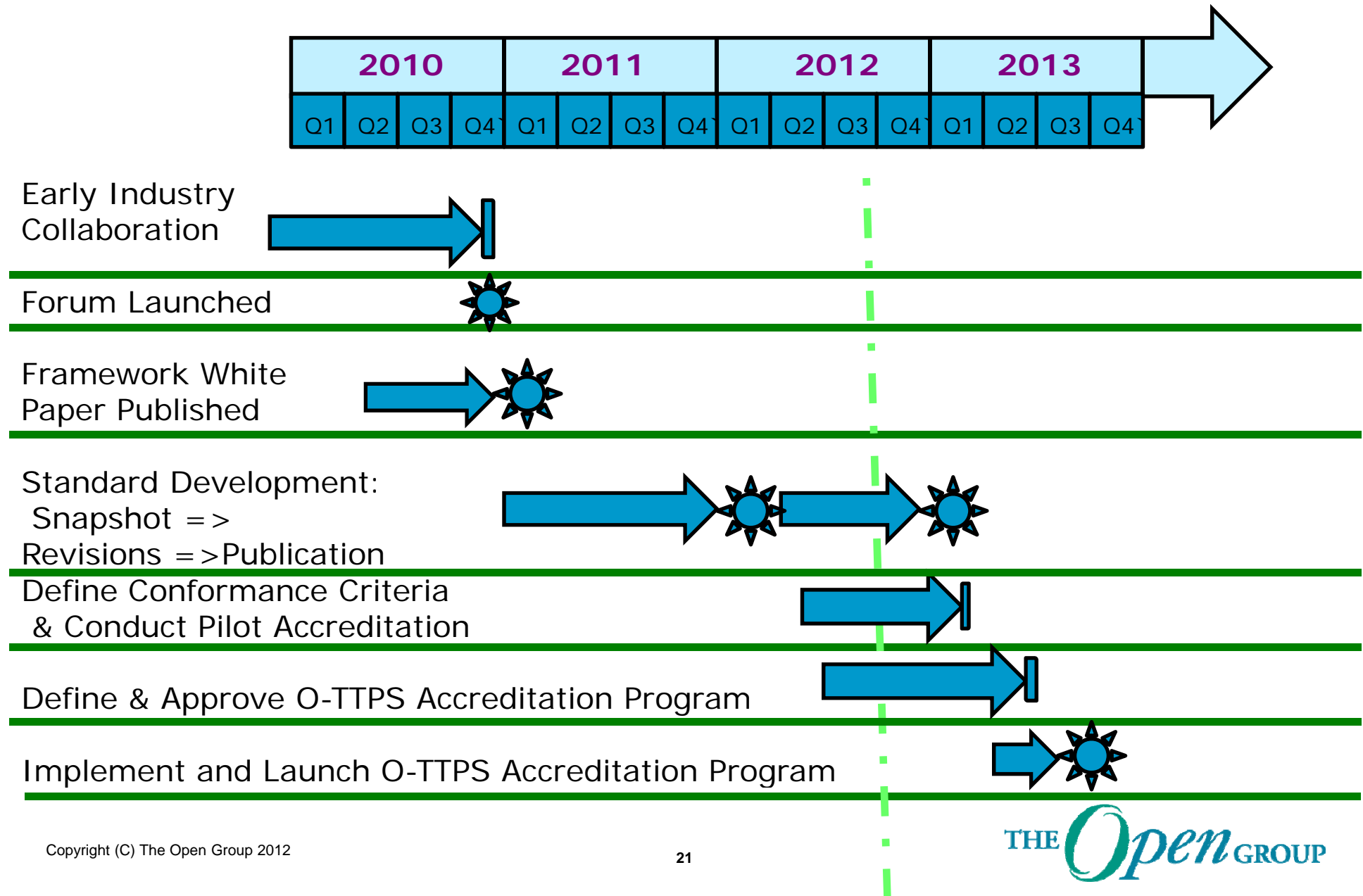
OTTF Standards Development Principles

- ❑ Our mission will be accomplished by providing providers, component suppliers, distributors, integrators and consumers commercially reasonable integrity practices that are:
 - **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
 - **Accreditation** – Organizational or process accreditation that is flexible enough that will allow for an organization to determine their own scope of accreditation – not intended to be an accreditation that is version specific to a product.

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



OTTF Milestones and DRAFT Schedule



Global Outreach and Harmonization

- ❑ **We know that for the O-TTPS Snapshot/Standard to have an impact - the standard must be adopted globally**
- ❑ **Moving forward on many fronts:**
 - Liaisons with ISO
 - Interfacing with NIST
 - Met with NSA and NIAP
 - Met with CESG (UK's country scheme equivalent to NIAP)
 - Met with various schemes (other countries) at CC Conference in Malaysia
 - Met with Senate and House staffers, Department of Commerce, Howard Schmidt
 - Met with government agencies in: Japan, UK, India
 - Outreaching through Open Group International Conferences: Taiwan, Brazil, Dubai, Australia, France, Sweden

Resources

- ❑ [The Open Group Trusted Technology Forum](#)
- ❑ [O-TTPS – Snapshot](#) released Mar 9, 2012
- ❑ [The Open Group represents OTTF at Congressional sub-committee hearing on Supply Chain](#) May 27, 2012
- ❑ [The O-TTPF White Paper](#) – serves as basis for the O-TTPF Best Practices currently under development
- ❑ [O-TTPF Vendor Testimonials](#)
- ❑ [OTTF Podcast](#) (Dana Gander with: Brickman, Lipner, Lounsbury, and Szakal)
- ❑ [The Open Group](#)

Benefits of OTTF

To Technology Providers:

- ✓Work collaboratively with peers, suppliers and customers to define, review, approve best practice approaches
- ✓Create a safer world by contributing to a more trustworthy global technology supply chain
- ✓Influence/require their sub-suppliers to follow the O-TTPF Best Practices
- ✓Direct interaction with government acquisition leaders
- ✓Gain a differentiation in the market through conformance and accreditation
- ✓Gain status as an organization by contributing to the development of the O-TTPF
- ✓Help harmonize global technology supply chain initiatives

To Customers:

- ✓Interact with providers in an open, neutral forum
- ✓Influence key technology providers and their practices
- ✓Vertical markets including government and defense, transportation, healthcare and financial services can have a collective effect on providing operational requirements for best practices that apply to their sector
- ✓Learn from the OTTF best practices, how best to improve the integrity of their enterprise, what to require of their component and service providers

Working Together to Raise the Bar Within the Global Supply Chain

- Join the discussion...
 - We welcome your participation!
 - We welcome your customers' participation!
 - We welcome your vendors' participation!
 - We welcome your component suppliers' participation!



Thank You!

O-TTPS Snapshot – Download it:

<http://www.opengroup.org/bookstore/catalog/s121.htm>

Read the Snapshot – provide comments at:

ogtff-admin@opengroup.org

For more information about the OTTF contact:

Mike Hickey m.hickey@opengroup.org

or

Chris Parnell c.parnell@opengroup.org