Open Trusted Technology Provider Framework (O-TTPF) Standard

The Open Group Trusted Technology Forum

“Build with Integrity

Buy with Confidence”™

Sally Long

Director, Consortia Services, The Open Group

Forum Director, Open Group Trusted Technology Forum

THE Open GROUP

Open Group Trusted Technology Forum

- ❑ Background on the OTTF
- ❑ OTTF Members and Structure
- ❑ The Supply Chain Challenge
- ❑ Responding to the Challenge
- ❑ Current Approach
- ❑ Best Practice Examples & Scoping Effort
- ❑ Timeline

About The Open Group's Collaboration Services

- ❑ A line of business within The Open Group
- ❑ Offering our proven tools and techniques
- ❑ Assist consortia to form and operate effectively throughout their full lifecycle

DOD and Collaboration Services

- ❑ Started with a Roundtable Discussion in Q4 of 2009
- ❑ Need to understand: What constitutes a “Good Commercial Product”
  - What if our goal is to simply acquire “good commercial products?” What does industry consider a “good commercial product”?
  - Vendors are making quality products – and in most cases secure and trusted products – so doesn’t it make sense to get together and establish best of breed best practices for industry?
  - Asked the vendors to do that and to consider a brand that would identify products from providers who implemented the best practices.

Need to Work Together on Defining Good/Trusted Products => OTTF

- ❑ "Trustworthy Commercial Product" – Helpful information that builds understanding of the 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 Expectations

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™*"

IBM

CISCO

ORACLE

Kingdee
金蝶，企业管理专家

Microsoft®

EMC²
where information lives®

hp

SAP

JUNIPER
NETWORKS

ca
technologies

NASA

Fraunhofer
SIT

IDA

APEXASSURANCE
GROUP

SAIC
From Science to Solutions

@sec
the information security provider

BOEING

DEPARTMENT OF DEFENSE
UNITED STATES OF AMERICA

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

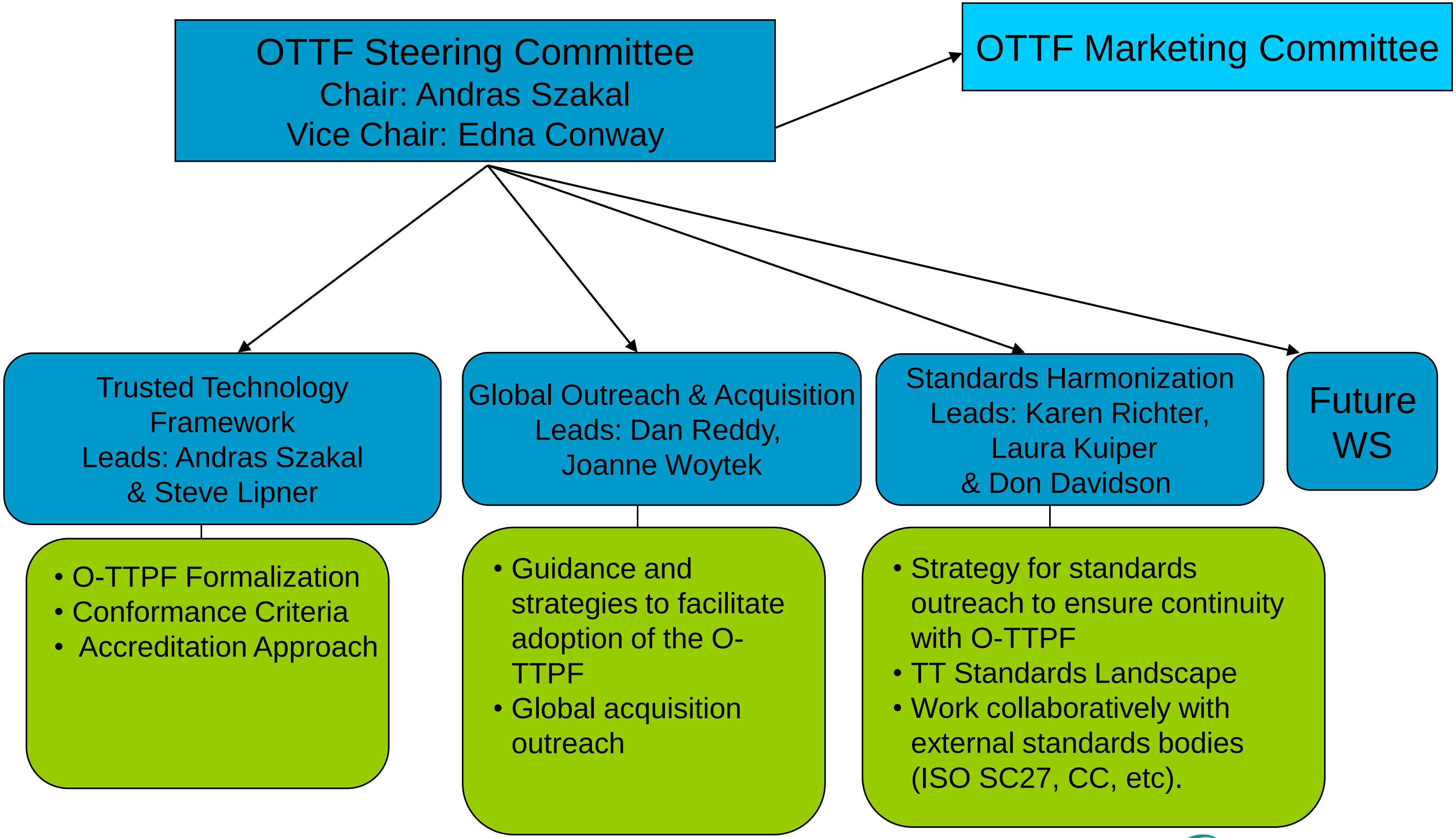
TATA
TATA CONSULTANCY SERVICES

MITRE

Software Engineering Institute | Carnegie Mellon

THE Open GROUP

OTTF Governing Structure (Current Work Streams and Committees)



OTTF Steering Committee
Chair: Andras Szakal
Vice Chair: Edna Conway

OTTF Marketing Committee

Trusted Technology Framework
Leads: Andras Szakal
& Steve Lipner

- O-TTPF Formalization
- Conformance Criteria
- Accreditation Approach

Global Outreach & Acquisition
Leads: Dan Reddy,
Joanne Woytek

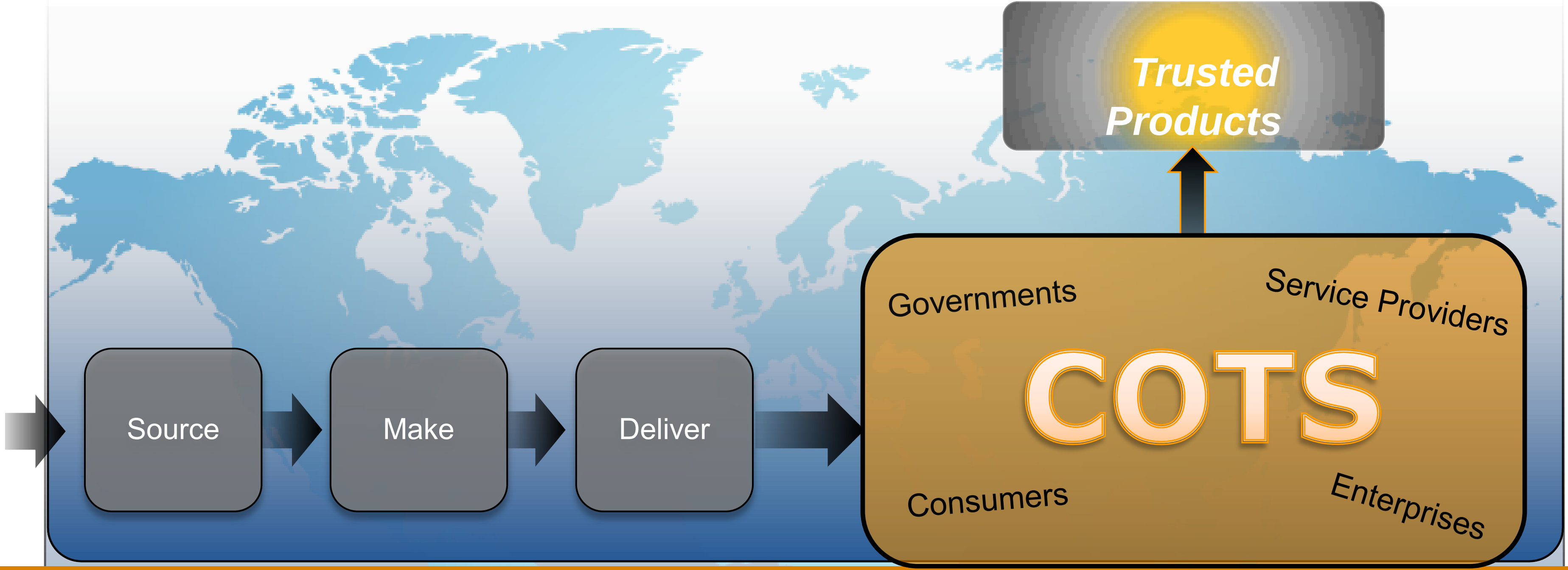
- Guidance and strategies to facilitate adoption of the O-TTPF
- Global acquisition outreach

Standards Harmonization
Leads: Karen Richter,
Laura Kuiper
& Don Davidson

- Strategy for standards outreach to ensure continuity with O-TTPF
- TT Standards Landscape
- Work collaboratively with external standards bodies (ISO SC27, CC, etc).

Future WS

The Challenge



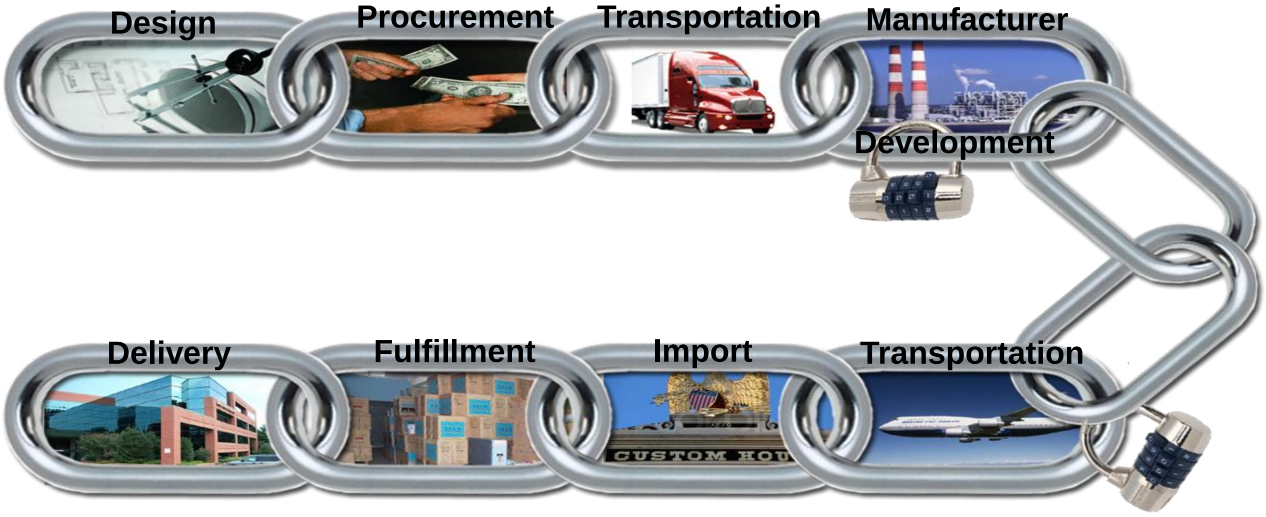
- ❑ COTS ICT come from the Global Supply Chain
- ❑ Addressing vulnerabilities requires a holistic view across the supply chain
- ❑ Complexity makes it difficult to assess risk for both customers and providers

No One Solution Addresses It All
Only Together Can We Succeed

Protecting the Technology Supply Chain

Risks From…

- Component Suppliers
- (within) Vendor
- Partners



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

How Is the Industry and Government Partnership under the Open Group Addressing These Challenges?

- Examining risks along the technology supply chain
- Capturing best of breed best practices used by industry to enhance security and integrity in COTS
  - The Open Trusted Technology Provider Framework (O-TTPF) - open standard that codifies best practices across the entire lifecycle covering:
    - Product Development
    - Secure Engineering
    - Supply Chain Integrity
- Evaluating how to use the O-TTPF 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

Current Approach

- **The OTTF currently plans to:**
  - stage the standard over time – with each stage addressing a set of threat models which map to one or more market needs
  - refine and refocus the scope of the framework to what will become the first version of the framework/standard:
    - for the first version we are looking at addressing best practices that help assure against counterfeit commercial technology products and tainted commercial technology products
  - develop a base set of objective and attainable conformance criteria
  - after completing the standard and conformance criteria, conduct an internal ”conformance pilot” to get some practical experience on whether and how to approach a verification program

Examples of O-TTPF Practices (Across the Supply Chain)

Refining scope for planned version 1.0 to identify best practices in each phase that help assure against tainted and counterfeit technology products

Trusted Technology Providers

Follow O-TTPF Best Practices

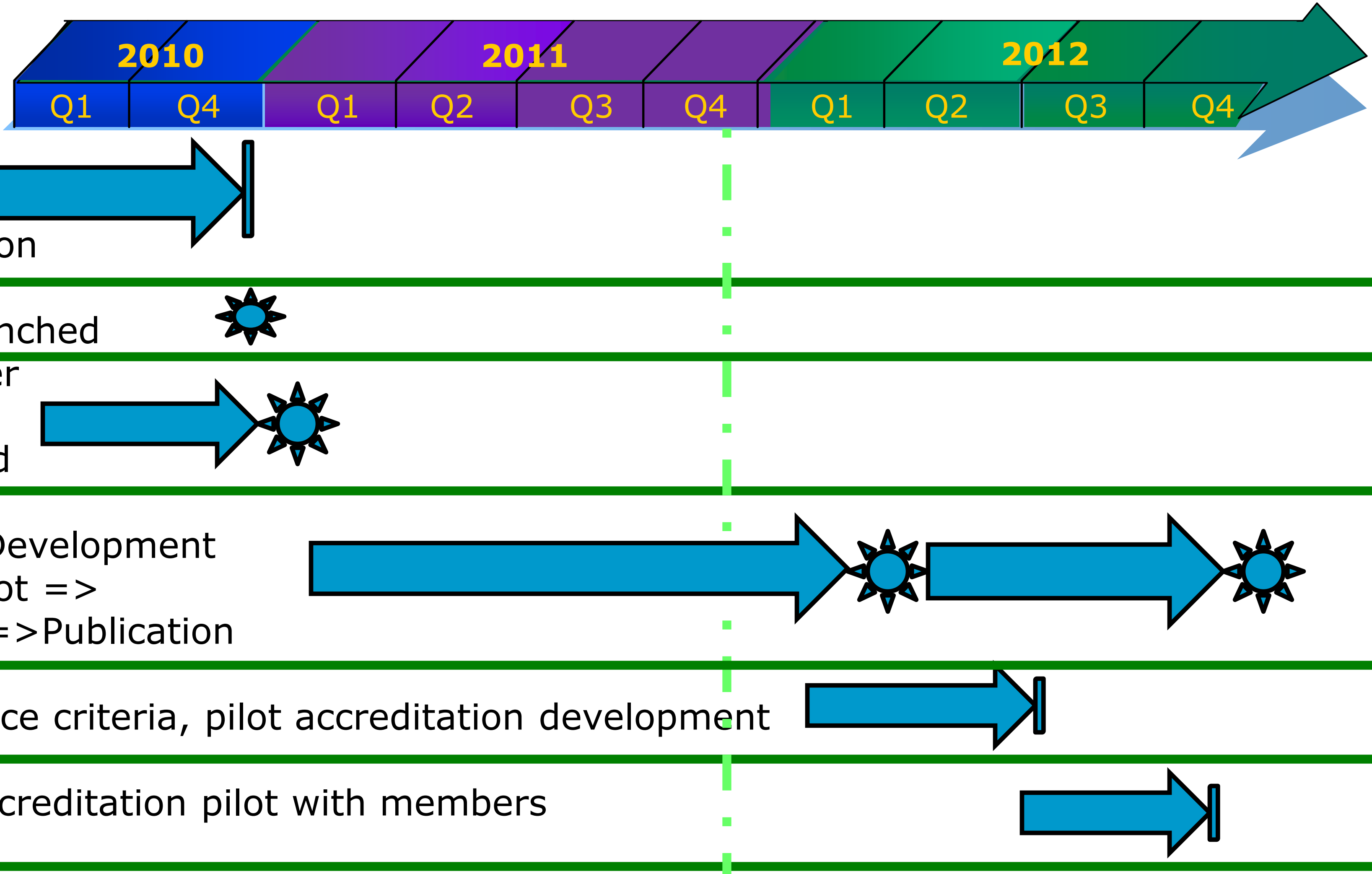
- ❑ Product Development
  - Well documented process and practices?
  - Trained professionals?
  - Do you formally manage requirements, design, etc.?
  - Quality test management?
  - Leverage software automation?
- ❑ Secure Engineering
  - Do you do threat modeling?
  - Secure code design reviews?
  - Risk assessment?
  - Tooling to minimize risk?
  - Do you digitally sign your code? Runtime protection?
  - Perform static code analysis?
- ❑ Supply Chain Integrity
  - Do your own sub-suppliers follow O-TTPF?
  - Do you verify components from suppliers?
  - Manage Open Source assets?
  - Protect against counterfeits ?
  - Do you have measurements for Employee and supplier security?
  - Business conduct guidelines?
  - Business Partners evaluated?
  - Do you have authorized service providers who follow O-TTPF?

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 Open GROUP

OTTF Milestones and DRAFT Schedule



Early Industry Collaboration

Forum Launched

White Paper Drafted & Published

Standard Development =>Snapshot => Revisions =>Publication

Conformance criteria, pilot accreditation development

Internal accreditation pilot with members

Global Outreach and Harmonization

- **We know that for the O-TTPF Best Practices to have an impact - the standard must be adopted globally – We are 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 though Open Group International Conferences: Taiwan, Brazil, Dubai, Australia, France, Sweden
- We don't want to get ahead of ourselves – so of utmost importance is completing the standard – more effective outreach and harmonization when there is something solid to share
- On the other hand we do want people to know we plan to deliver a standard and to come and join us in that work or in our harmonization work

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.”*

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 suppliers’ participation!

Thank You!

Please contact
Mike Hickey or
Sally Long for more information
m.hickey@opengroup.org
s.long@opengroup.org

THE Open GROUP

Background Slides

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

Resources

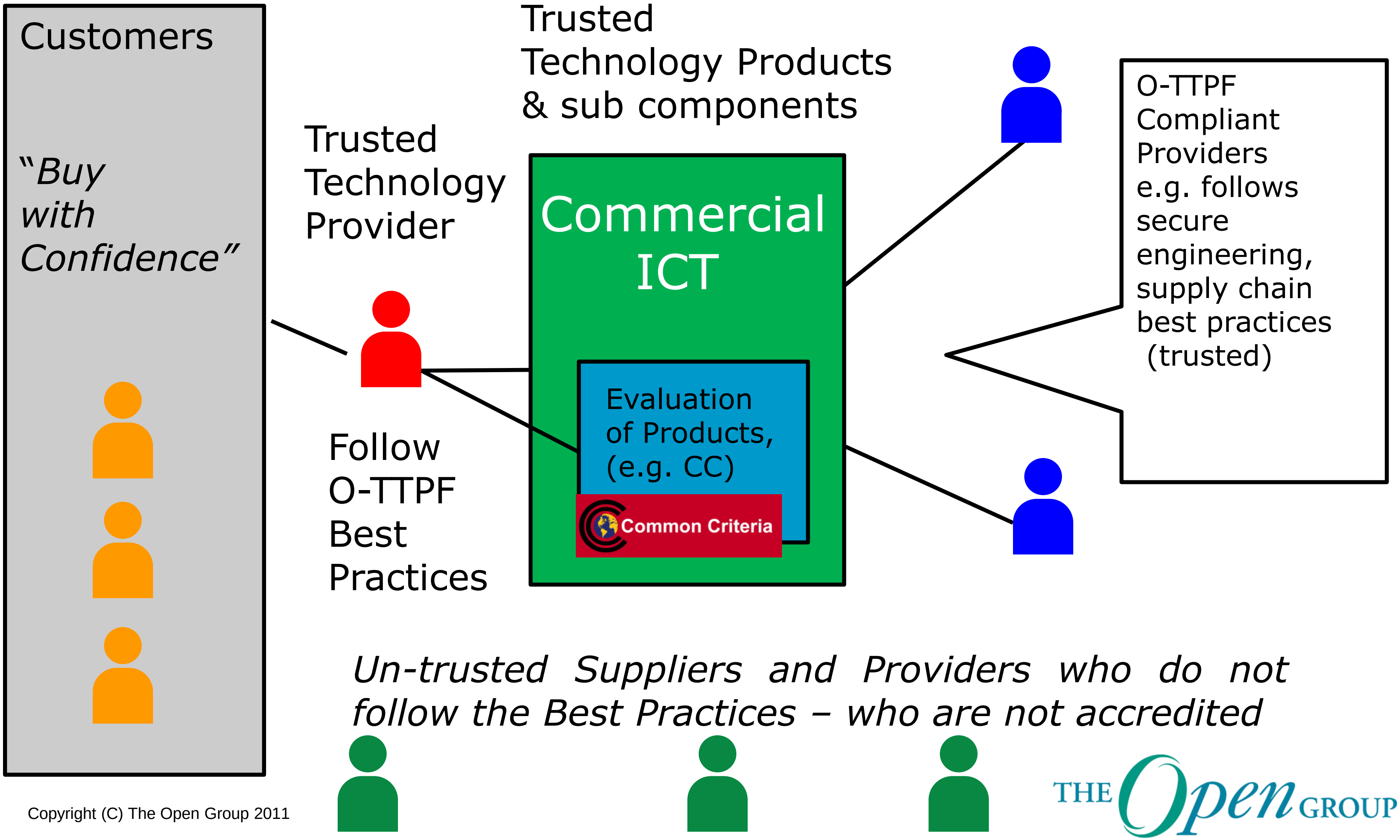
- The Open Group Trusted Technology Forum
- The O-TTPF White Paper – serves as basis for the O-TTPF Best Practices currently under development
- O-TTPF Vendor Testimonials
- Recent OTTF Podcast (Dana Gander with: Brickman, Lipner, Lounsbury, and Szakal)
- The Open Group

OTTF Standards Development Principles

- Our mission will be accomplished by providing vendors, 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.

Customers Buy with More Confidence:

Providers & Suppliers Can Extend Supply Chain Integrity



Customers

"Buy with Confidence"

Trusted Technology Products & sub components

Trusted Technology Provider

Commercial ICT

Evaluation of Products, (e.g. CC)

Common Criteria

Follow O-TTPF Best Practices

O-TTPF Compliant Providers e.g. follows secure engineering, supply chain best practices (trusted)

Un-trusted Suppliers and Providers who do not follow the Best Practices – who are not accredited

THE Open GROUP