Purchasing more secure ICT products and services

EastWest Institute ICT Buyers Guide

https://www.eastwest.ngo/i dea/eastwest-institute-launches-cybersecurity-guide-technology-buyers

EastWest INSTITUTE

Andy Purdy, Chief Security Officer, Huawei Technologies USA

Kaja Ciglic, Senior Cybersecurity Strategist, Microsoft

AGENDA

Supply chain cybersecurity

Overview of EWI Buyer’s Guide

Path forward

The EastWest Institute (EWI)

- An independent NGO that works to reduce international conflict, addressing seemingly intractable problems that threaten world security and stability.
- Recognized and trusted for its unique capacity to bring together key policymakers, experts, business leaders and innovators—forging new connections, driving dialogue and introducing sustainable solutions.

Threats to global supply chains

Courtesy of The Open Group

Stakeholders / Main Threats	Tainted		Counterfeit	
	Upstream	Downstream	Upstream	Downstream
Malware	√	√	√	
Unauthorized “Parts”	√	√	√	
Unauthorized configuration		√		
Scrap/Sub-standard Parts			√	
Unauthorized Production			√	√
Intentional Damage	√	√		

Confidentiality Integrity Availability Traceability Authenticity

The supply chain challenge

Assurance best practices need to replace product certification and be applied throughout its lifecycle and supply chain.

Source

Make

Deliver

Secure in-house development and global supply chains requires:

- A security life cycle approach
- Best practices for all constituents in the supply chain
- Common requirements and international standards backed by assurances
- A public registry to identify trusted providers
- Customers attuned to concerns, so that they reward trusted constituents through procurement

KEY POINTS

This Buyers Guide is intended to help the buyers, suppliers, and users of information and communications technologies **better understand and address** the cybersecurity and privacy risks inherent in ICT products and services.

Greatest incentive for providers to raise the bar for **cybersecurity assurance,** is if it’s required by informed buyers.

Buyers of ICT need risk-based security requirements for their procurements, and to use their **collective purchasing power** to incentivize raising the security bar.

The Guide provides these **three overarching recommendations** for ICT buyers and suppliers:

1. Engage in a dialogue about risk management.
2. Use the Guide to frame the dialogue
3. Rely on international standards to increase confidence in the results.

OVERVIEW

Enhancing cybersecurity globally by enabling the availability and use of more secure ICT products and services

.

1. ICT buyers should engage in a dialogue about risk management – with like-minded buyers and potential suppliers, and with government and private sector stakeholders.
2. The insights and questions in the Buyers Guide can help frame the dialogue and inform procurement requirements.
3. Whenever possible, reference international standards in setting requirements.

Supply side

- Promote use of international standards and best practices for product and service integrity
- Facilitate approaches for more informed conversation between suppliers and buyers

Demand side

- Foster use of procurement practices based on common requirements, international standards and best practices for secure ICT
- Work to prevent trade barriers so buyers can identify and utilize trusted providers regardless of locale

PRINCIPLES

Guiding roles and responsibilities of stakeholders involved

Actor	Government		Industry
Role	Policy maker	ICT Buyer	ICT Provider
Five Principles			
Maintain an **open market** that fosters innovation and competition and creates a **level playing field** for ICT providers	√		
Create procurement practices that utilize **fact-driven, risk-informed, and transparent requirements** based on international standards and approaches		√	
Avoid requirements or behavior that **undermines trust** in ICT (e.g., by installing back doors)	√		√
Evaluate the practices of ICT providers in terms of creating product and service integrity		√	
Create and use tools and approaches to **address risk** and **assign high value** to cybersecurity investments	√	√	√

CORE STRUCTURE

Three essential components of secure procurement

Enterprise security governance

- Strategy and control
- Standards and processes
- Human resources

Security across product and service lifecycle

- Design and development
- Build
- Release, fulfillment, and distribution
- Sustainment and response
- Sourcing and supply chain

Creating assurance

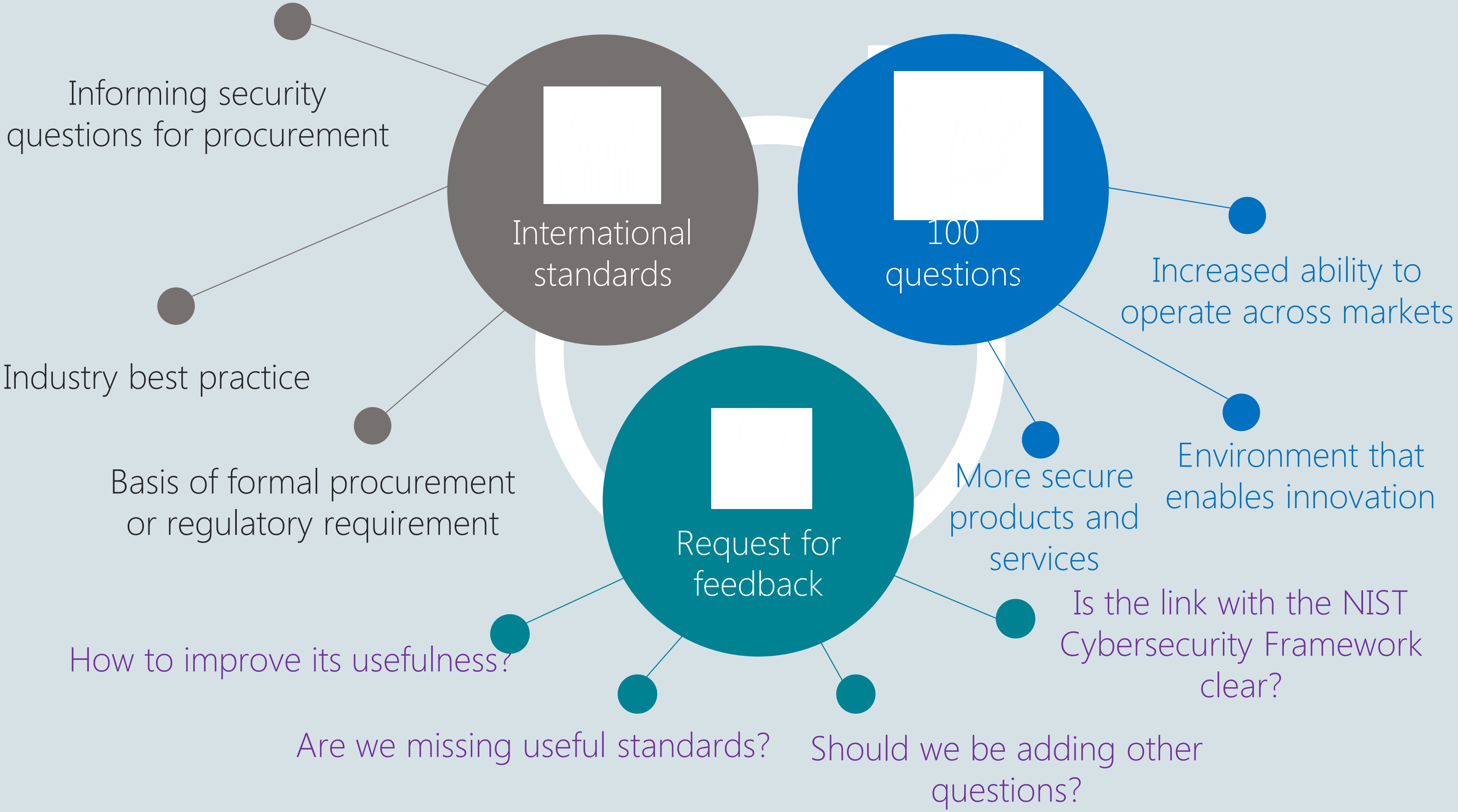
Fostering Assurance

- Laws and Regulations
- Contracts
- Transparency

Demonstrating Assurance

- Self Attestation
- External Attestation

APPENDICES:
A critically important part of the guide


Informing security questions for procurement
Industry best practice
Basis of formal procurement or regulatory requirement
International standards
100 questions
Increased ability to operate across markets
More secure products and services
Environment that enables innovation
Request for feedback
How to improve its usefulness?
Are we missing useful standards?
Should we be adding other questions?
Is the link with the NIST Cybersecurity Framework clear?

Summary

Comprehensive risk management: Organizations should address the risks to their supply chains as part of a comprehensive risk management program.

Common requirements: Buyers should recognize most security risks are common and therefore utilize common procurementt requirements. Upon risk assessments they should determine their unique delta.

International standards: Use of international standards are critical to increasing security of ICT.

Purchasing power: Organization should leverage their purchasing power to drive responsible security behavior with their vendors.

Partner: Finally, how can we work with ITU to move these principles forward?

The Hague Centre for Strategic Studies

EastWest Institute

NXP

VimpelCom

Microsoft

HUAWEI

The William and Flora Hewlett Foundation

IEEE Communications Society

Munich Security Conference msc Münchner Sicherheitskonferenz

Sonus

Unisys

CenturyLink

paloalto Networks

The Open Group

360

For more information:
Andy Purdy, Huawei (andy.purdy@Huawei.com)
Kaja Ciglic, Microsoft (kaja.ciglic@Microsoft.com)
Bruce McConnell, East West Institute (bwm@ewi.info)

https://www.eastwest.ngo/idea/eastwest-institute-launches-cybersecurity-guide-technology-buyers

Relevant International Standards Appendix A – The O-TTPS Example

The Open Trusted Technology Provider Standard

- Best Practices for product integrity and supply chain security
- Developed by consensus of the OTTF approved as ISO/IEC 20243 in 2015
- Certification program for formal recognition of ICT providers (e.g., OEMs, hardware and software component suppliers, value-add resellers, etc.) who conform
- Certification program now has two levels
  - third-party assessed (current)
  - self-assessed (available in Dec, official announcement in January)
- Both levels backed by warranty – if found not to be conformant later, certificate removed from public registry – till they fix the problem.
- Customers can decide what level to ask for in procurement based on acceptable risk for their application and operating environment

Relevant International Standards recognized in survey results

- Standards related to Governance and Risk Assessment:
  - ISO 27001 and 27002
  - ISO 27005
  - NIST Cybersecurity Framework (Framework references stds)
  - Open Fair (Risk Analysis Methodology)
- Standards related to Product and Services Life Cycle
  - NIST 800-53
  - NIST 800-161
  - ISO 20243
  - ISO 27034
  - ISO 27036
- Please see Appendix A for list of additional standards
- EWI welcomes suggestions of other standards for inclusion