



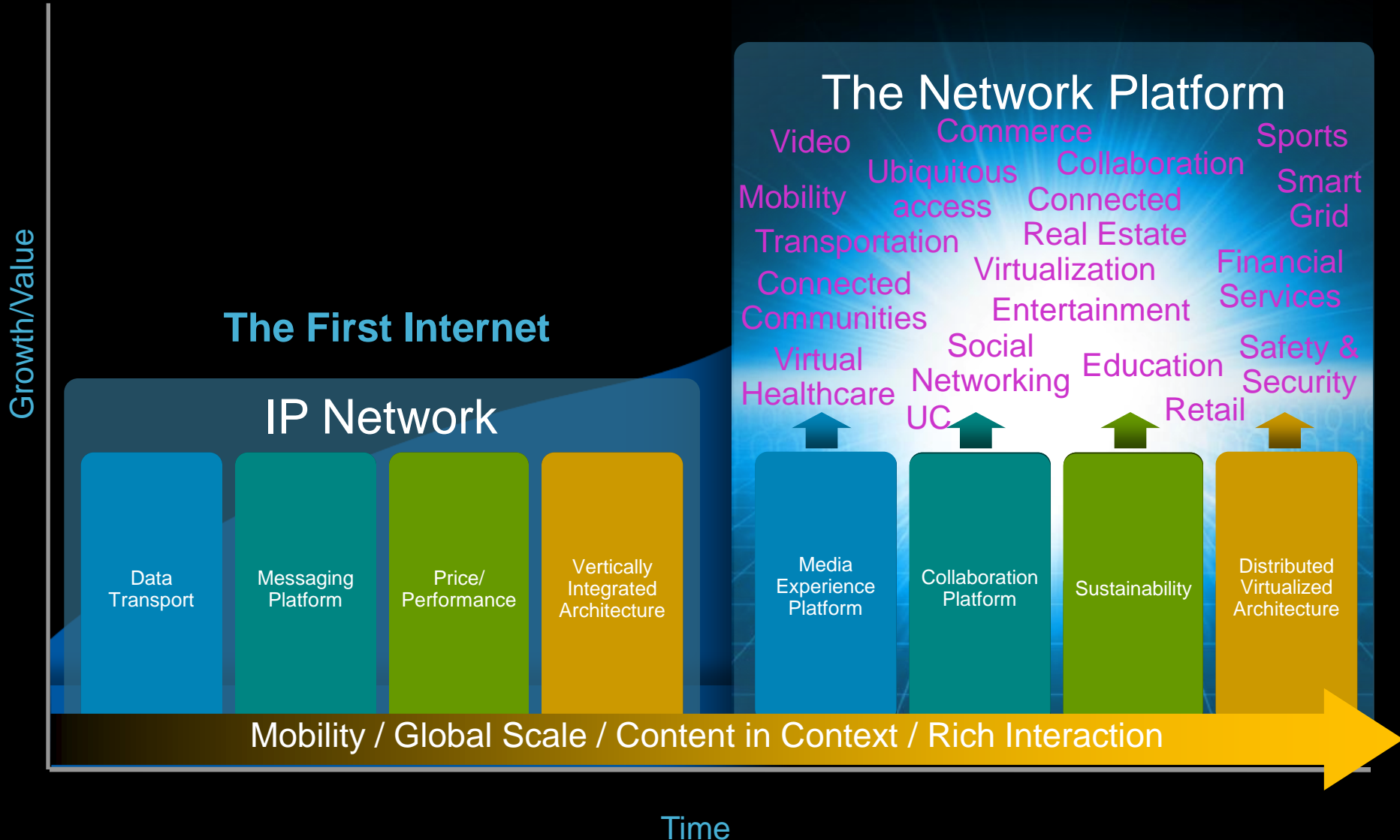
Common Criteria – An Industry Perspective

Embrace, Reform, and Extend

Gene Keeling
Director, Global Certification Team

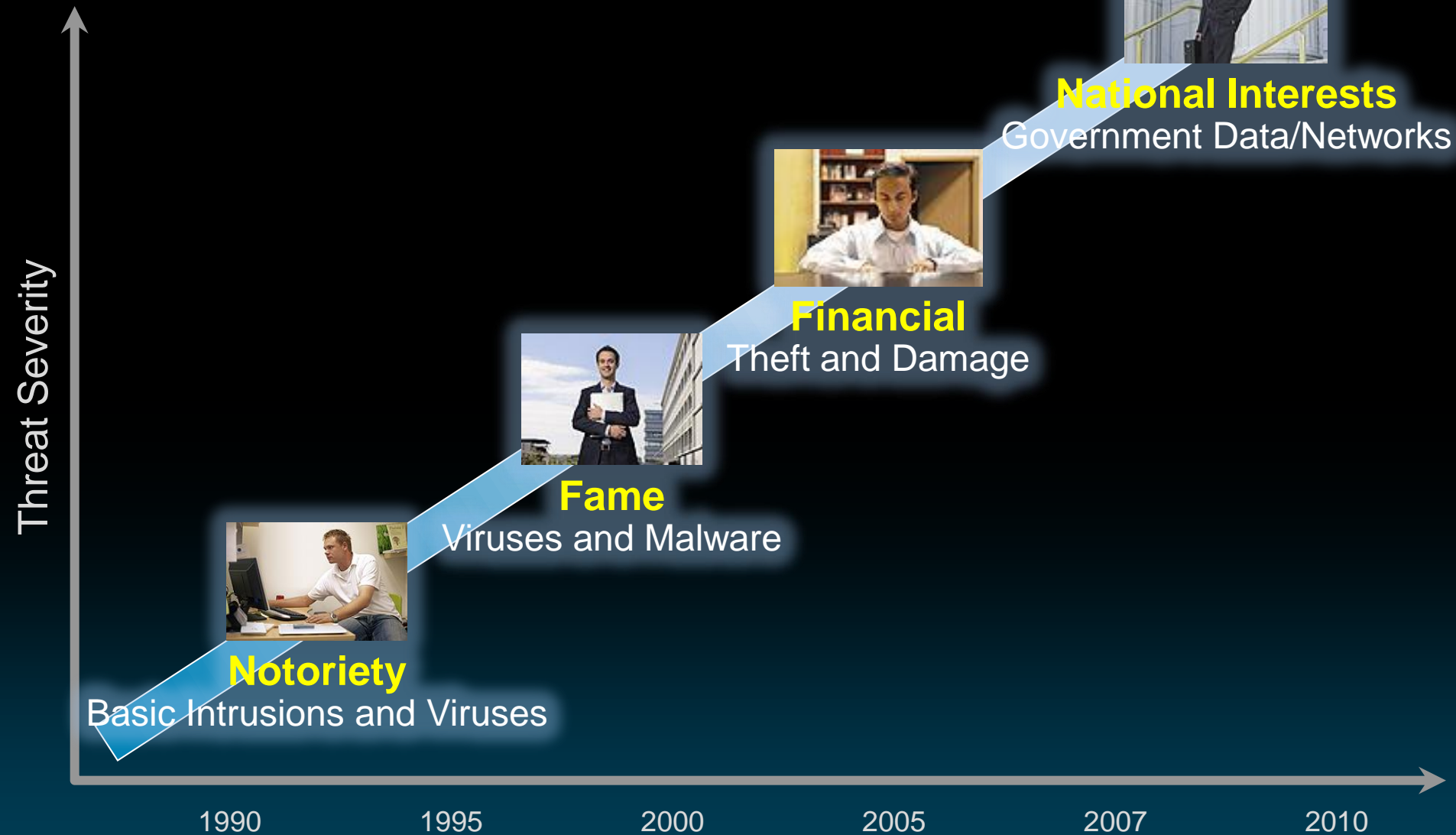
Evolution of the Internet

The Next Internet



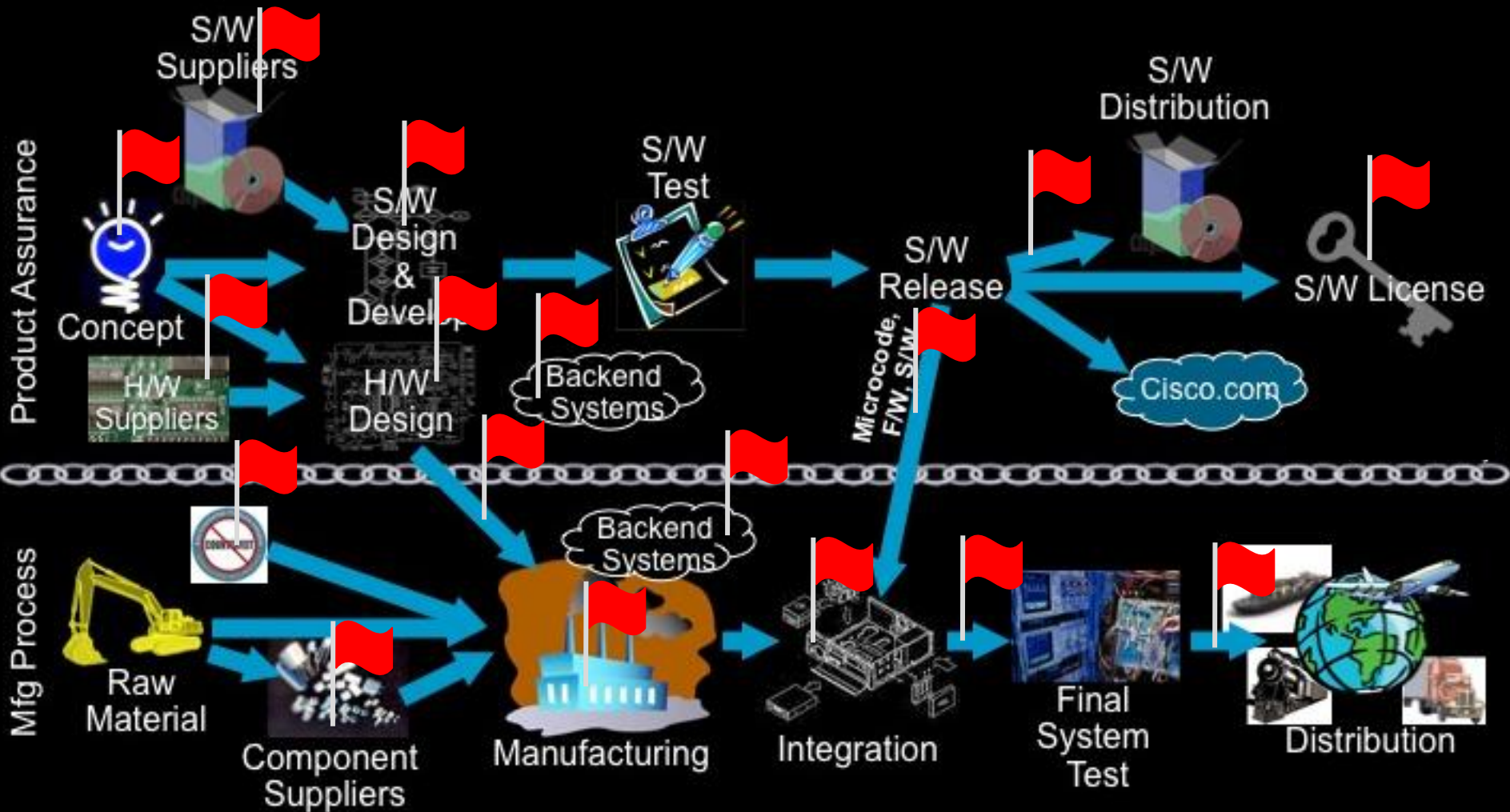
Evolving Threats

Increasingly Difficult to Detect and Mitigate



Newest Concern

“Supply Chain” Security and Threats



Importance

One network

+

Increasing reliance on information technology

+

Increasing financial and strategic opportunities
associated with cyber exploits

=

Greatest opportunity for Common Criteria
to be more relevant than ever before

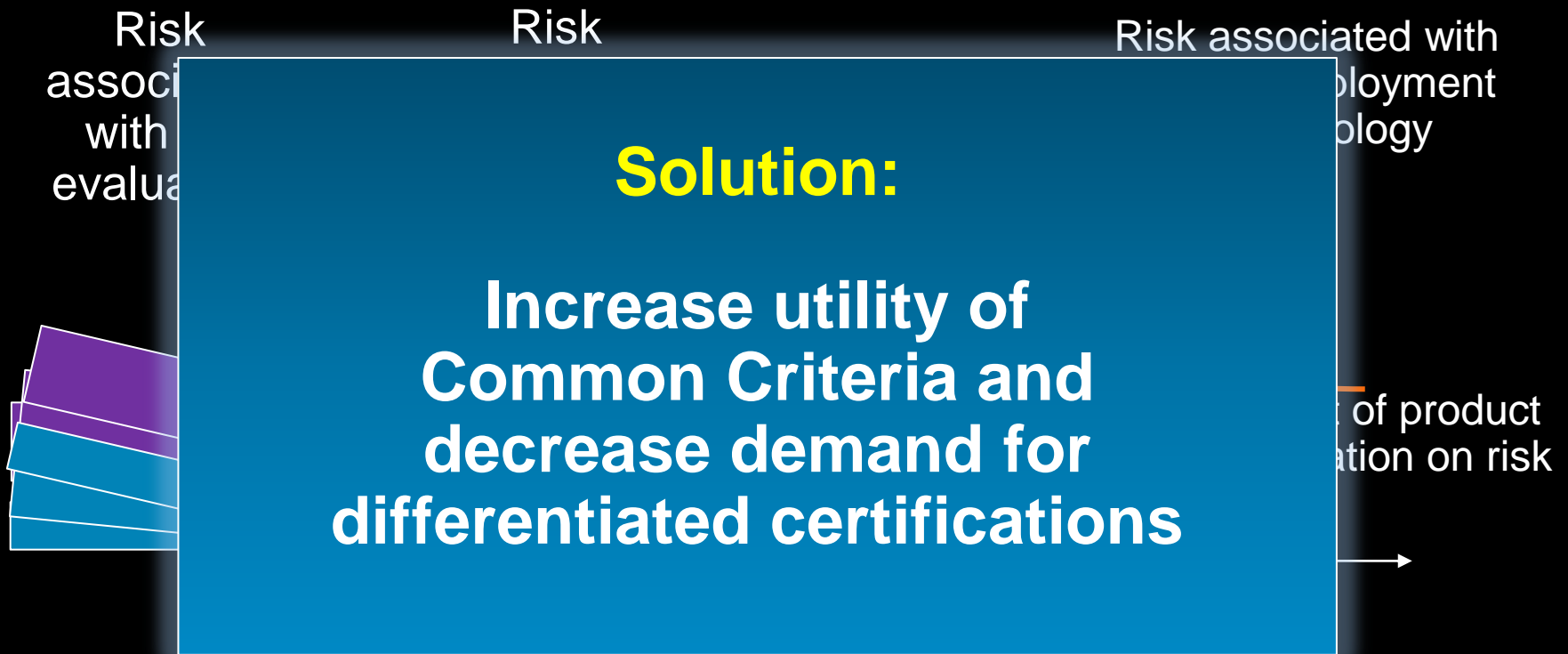
Certification Challenges

- Government customers are relying on COTS products more than ever before
- Technology continues to evolve at an ever increasing rate
- Threats (number, type, sophistication) continue to evolve

Government Response:
Increased Focus on Certifications

Security Inversion Inflection Point

Time and Innovation Matter



As organizations create unique certification requirements, cost and time-to-market increase dramatically as does risk

Cisco's Analysis for Next 24 Months

- Number of products to be certified will **double**
- Number of certifications required will **quadruple**
- Assumes Common Criteria remains mutually recognized

**Common Criteria is key to industry
being able to scale to meet the
needs of government customers**

What To Do About Supply Chain Security?

Product Assurance + Manufacturing Process Integrity

IT Customers
Globally

Government Customers
Globally

Need to
build

Standards-based, mutually
recognized accreditation
process (ISO-like)

Need to
expand

Common Criteria
(mutually recognized
certification process)

Accreditation vs. Certification will be a function of customer
as well as product type and will change as threats mature

Industry Needs to Step Up!

- Industry must take on a greater role
- We must be pro-active
- We must socialize the benefits of Common Criteria
- We must build on the mutually-recognized, international standards that exist today

Embrace and Extend

People Ask: “What Do You Suggest?”

- Focus on realistic, achievable goals
- Look for the “low hanging fruit”
- Identify what can be delivered within next 12 months
 - We’ll add more later
- Leverage CCVF

Stop Talking, Start Doing

Customer Challenges

- Assurance the product does what they need it to do
- Greater requirements
- Assurance against today's emerging threats
- Assurance the vendor development and manufacturing processes protect against today's emerging threats, including
- Need to address some country-specific and lower assurance needs that are not being met by CC

Protection Profile Development

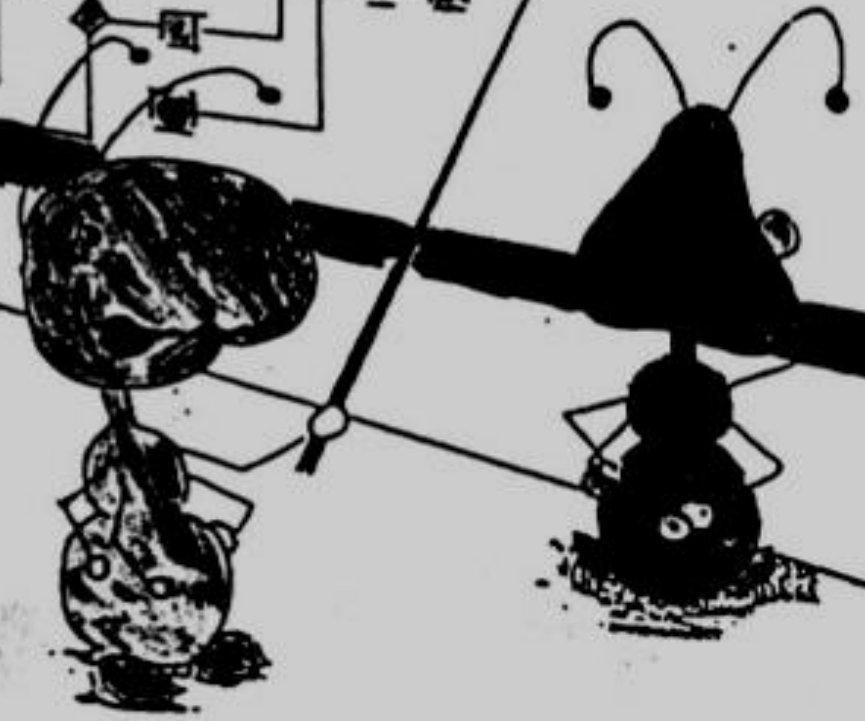
Improve Efficacy of Evaluations

The Proposal

Common Criteria Process



Good work,
but I think we might
need just a little more
detail right here.



Protection Profile Development

Key Deliverables

- Set of **protection profiles** that reflect global customer security needs
- **Disciplined process** to develop PPs with standard milestones and deliverables **that improve transparency and visibility**
- Clear **roadmap** of PP development and open mechanism to **report development status** based on standard milestones to all stakeholders
- Practical **transition/sunset plan** for current PPs to new PPs

Improving Evaluation Efficacy

Key Deliverables

- A set of **evaluation activity requirements** that ensure timely, consistent and relevant CC certifications
- A set of **vendor evidence requirements** that ensure timely and relevant CC certifications
- A set of **vendor development, delivery and life cycle support processes** that ensure the robustness of product security throughout the supply chain and product lifecycle
- A practical mechanism to **leverage evaluation results** from one product version to the next and across products using shared development processes

How We Can Move the Needle Together

- **Cisco**

- Continue to co-lead firewall PP development

- Drive towards more disciplined schedules and deliverables

- Join in an effort to bring together all stakeholders to review the current assurance requirements against current customer needs

- **CCVF**

- Promote activities that address vendor and customer concerns

- **CCDB**

- Collaborate and encourage all stakeholders to participate

- Socialize the benefits of Common Criteria and mutual recognition

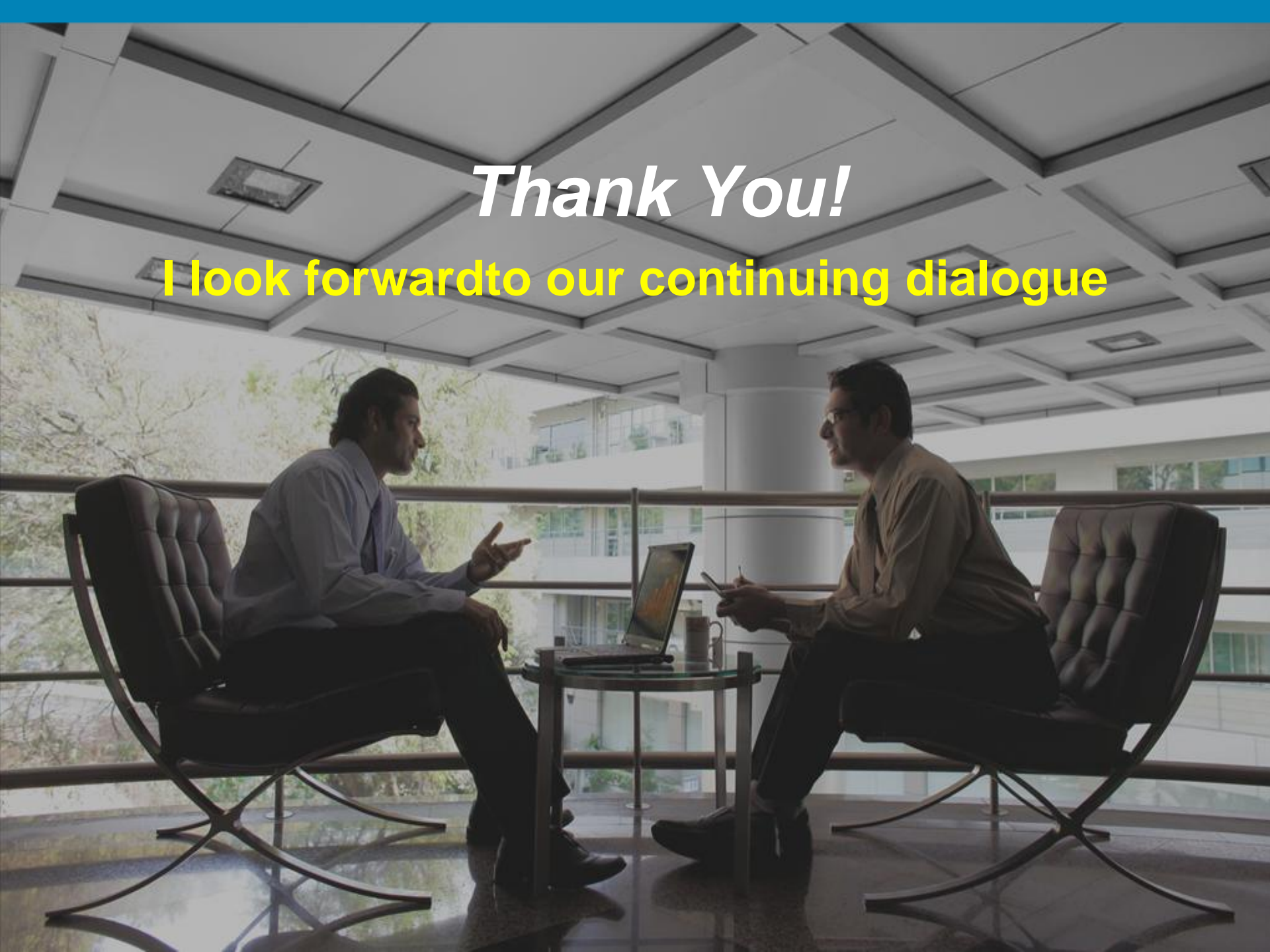
Closing Thoughts

- We are at an inflection point for Common Criteria
- Common Criteria is more relevant today than ever before
- Common Criteria is the only way for industry to scale to meet customer needs
- Industry must take a greater role in the reform effort
- Let's focus on realistic, near-term, achievable goals

We've Got to Get it Right

Thank You!

I look forward to our continuing dialogue





Protection Profile Development – Detailed Action Plan

- Identify and invite key stakeholders to participate in PP development.
- Review and vet the set of PPs to be developed.
- Plan the “roadmap” of PPs to be developed based on available resources and priorities.
- Adopt and adapt a disciplined PP development process with well-defined milestones and deliverables.
- Identify and implement collaboration and communications mechanisms and tools for PP development team interactions.

Protection Profile Development – Detailed Action Plan (cont.)

- Identify contributors/participants and develop the prioritized list of PPs
- Leverage existing customer requirements documentation such as DISA/NATO Security Technology Implementation Guides (STIGS) and ICOSA Labs test criteria and include these in the PP security functional requirements (SFR).
- Review NIAP's Common Requirements and applicability to PP development.
- Clearly understand and define the threats that are being addressed and ensure those threats are realistic and recognized by customers.

Protection Profile Development – Detailed Action Plan (cont.)

- Ensure each PP development team publishes status in accordance to the standard major milestones described by the standard development process.
- Develop realistic transition plans to migrate from existing PPs to updated PPs.

Improving Evaluation Efficacy – Detailed Action Plan

- Identify and invite key stakeholders to participate in this effort.
- Weigh the security assurance requirements (SAR) in CC Part 3 and the Common Evaluation Methodology (CEM) against customer needs and expectations versus time and effort to evaluate.
- Replace ineffective evaluation efforts with more value-added, efficient efforts.
- Eliminate duplicated evaluation effort that add no customer value by leveraging other ISO (e.g. systems engineering) standards and focus CC solely on security.

Improving Evaluation Efficacy – Detailed Action Plan (cont.)

- Identify more quantitative evaluation measures that can replace the qualitative measures taken today.
- Identify the current vendor assurance measures and ensure that the key measures that reflect customer requirements are included in the CC evaluation.
- Increase leverage across evaluations by examining and enhancing:
 - Continuity assurance
 - Site certification
 - Predictive assurance

Improving Evaluation Efficacy – Detailed Action Plan (cont.)

- Enhance the breadth of current SARs to address current security issues (e.g. code vulnerabilities and supply chain)
- Develop a set of assurance packages and supporting documents and/or recommendations for CC Part 3 and CEM standards modifications to support the more effective, relevant and efficient SARs

