RSA CONFERENCE 2014
FEBRUARY 24 – 28 | MOSCONE CENTER | SAN FRANCISCO

Share.
Learn.
Secure.
Capitalizing on
Collective Intelligence

Riding the Tiger – Harnessing the Power of Industry in Cyber Security

SESSION ID: PNG-W04A

David Martin
Head of International Assurance
CESG (UK Government)
@ccdbinfo

Dag Stroman
Managing Director FMV/CSEC,
FMV (Swedish Government)

What is Common Criteria? and where does it fit in?

- International Standard for IT Product Security Assurance
- The basis for ISO/IEC 15408 and ISO/IEC 18045
- CCRA - Recognition Arrangement between 26 Nations
- Can provide a common foundation level for procurement
- Aim - Evaluate once, use in many countries

Increasing effectiveness, relevance, and role

Industry changes

- Many new technologies
- Many development approaches
- Short time to market
- Frequent updates
- Wide range of attackers

Government/User needs

- Information for more products
- Accuracy and comparability
- Industry Standards
- Benefit from Industry Expertise (and effort)

Common Criteria

What is changing?

- Supporting wider standardisation via Collaborative Protection Profiles (**cPPs**)
- Greater industry involvement
  - Via Common Criteria User Forum (CCUF)
  - Via International Technical Communities (**iTCs**)
- Increased transparency, repeatability, effectiveness
- Supporting stronger links to procurement and users/specifiers

How is it changing?

- New Recognition Arrangement (CCRA) drafted
- Encourages use of cPPs and iTCs
- 36 month transition after ratification (expected this year)
- Close working with Common Criteria User Forum (CCUF)
- Collaborative Protection Profile process
- Supporting stronger links to procurement and use

Debunk a myth - 4 is better than 2

- iTCs can propose the use of assurance activities above those currently in the level ‘EAL2’
- The expectation is however that these would be rare
- Outside of cPPs, the recognition level will be limited to activities in EAL2 and below.
- “But surely 4 is bigger than 2?”

Debunk a myth - 4 is better than 2

- Well, yes, arithmetically, 4 > 2
- But is bigger, really ‘better’ in CC?
  - Often not in current practice
  - iTCs are free to demonstrate the value and how to fairly manage additional activities (transparency, repeatability, etc)
- The activities involved in EAL1 and EAL2 provide major benefits when combined with a detailed common spec (cPP) and the lower cost and faster speed is much more effective for cyber defence
- Let’s move away from ‘silly marketing’ mostly based on EALs

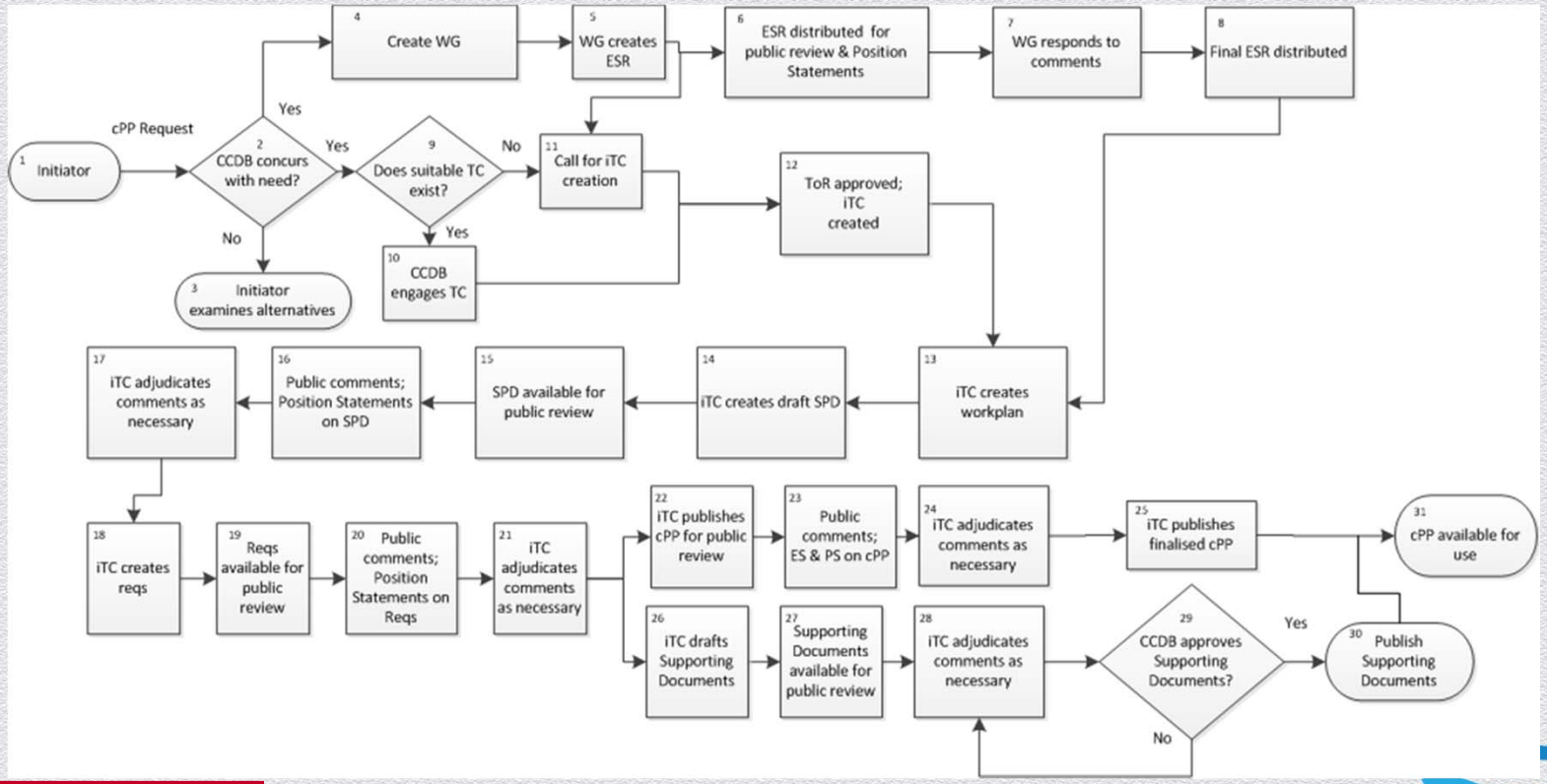
The iTC/cPP Process – Aims

- Uses available skills and effort effectively:-
  - Industry ‘has the pen’ for the standard
  - Users (e.g. Government) can steer the direction
  - CCRA guides recognition aspects
- Open and Transparent (obeys World Trade Organisation principles for open standards)
- Improves via feedback loops
- Continuous and agile (keeps standards up to date)

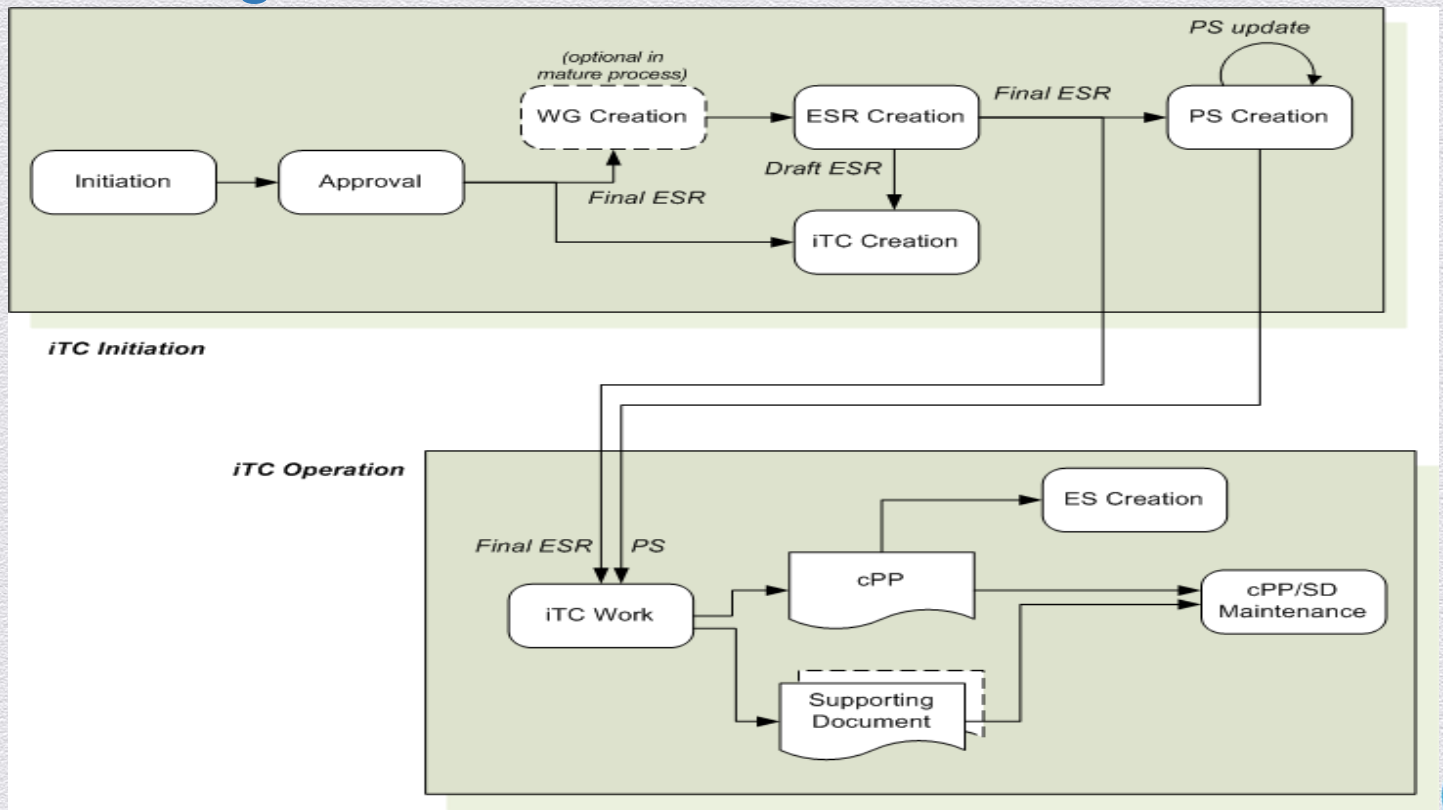
Warning! – Here comes ‘The Beast’

- Look away now if you have a nervous disposition
- We want to show the draft process
- But only to quickly point out the many points for interaction
- The number of steps will reduce over time
- There is no memory test at the end of the talk!
- (But we are happy to explain more in the hallway)

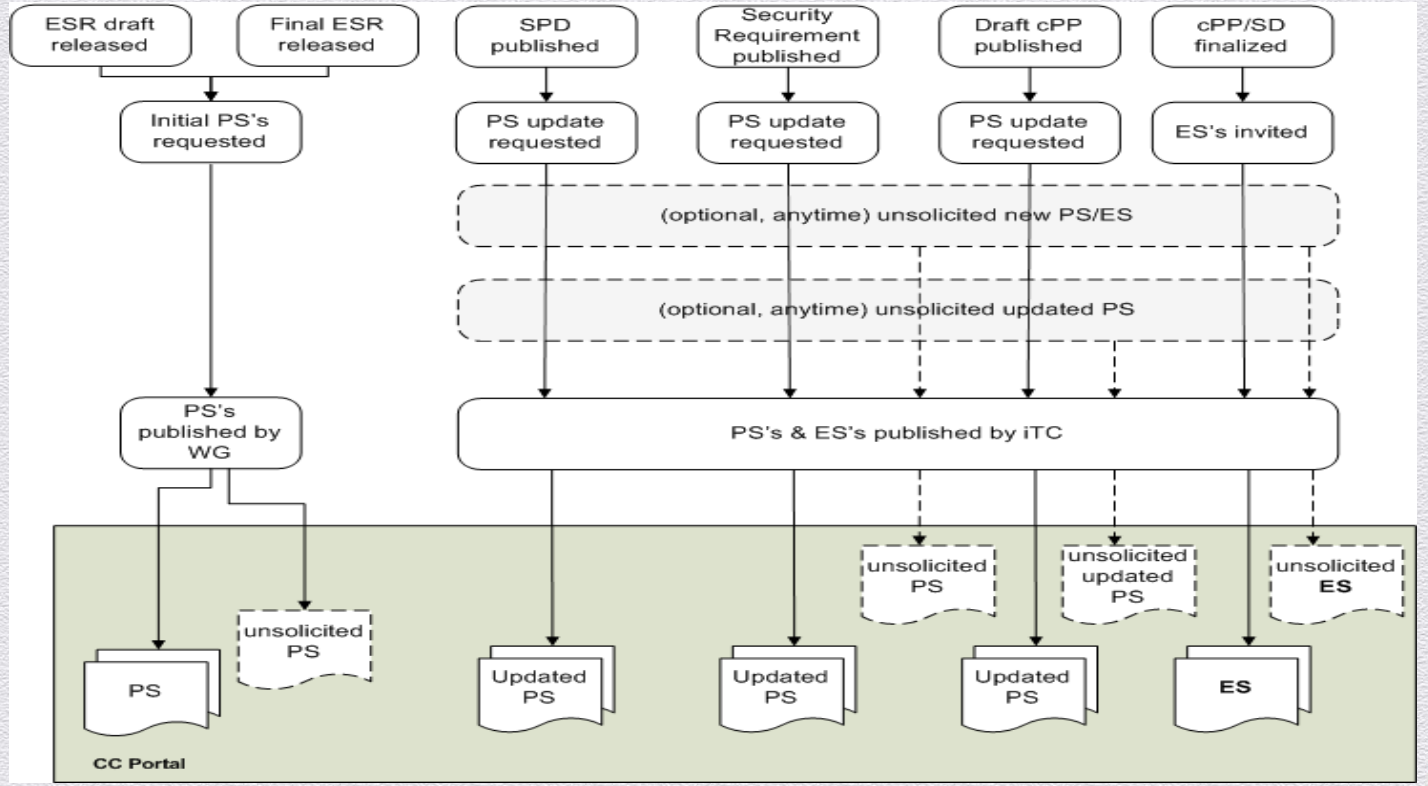
Draft cPP Process



Breaking it down a bit



Interaction and Guidance



The iTC/cPP Process – Key Points

- Strong links to Procurement/Requirements
- Results in effective, agile, standards
- Technical Communities provide continual relevance and improvement
- Uses available skills and effort effectively
- Harnesses the power of industry
- ‘Riding Tigers’ NOT ‘Herding cats’
- Come and take part!

Common Criteria

Debunk a myth - Recognition = procurement?

- Surely if my product is ‘recognised’ in 26 countries they will all buy it anyway?

Debunk a myth - Recognition = procurement?

- ‘Recognition’ means that a CC Participant ‘recognises’ that the certifying body correctly performed all of the activities involved in the CC (and CCRA) processes
- It does not mean that the product meets any needs of that nation
- But vendors sometimes think that this is the implication
- That is why it is important to adapt and to define common standards (cPPs) and supporting mechanisms (e.g. Position Statements/Endorsement Statements) that can help clarify procurement

Common Criteria

Debunk a myth - CC is full of Goobledegook

- I get lost in all the ‘Three Letter Abbreviations’, rules of combination, etc.
- But obviously I still need clarity and precision around what I am buying/using
- Can that be improved?

Debunk a myth - CC is full of Goobledegook

- The draft cPP process described will use plain language at all stages
- Early stage documents are all/mostly plain text
- Later stages (e.g. the cPP itself) will use CC language
- BUT with extensive plain text around each element
- Can that be further improved? – Come and help!

Debunk a myth - Vendors will cause a 'race to the bottom' in cPPs

- Much of the work in iTCs will be done by vendors.
- Greatly reducing the functionality to be evaluated and the activities involved could result in much lower evaluation costs
- Therefore the 'nasty' vendors will 'conspire' to do this!

Debunk a myth - Vendors will cause a 'race to the bottom' in cPPs

- Government CC Schemes will be involved in iTCs,
- As will evaluation experts (from labs and schemes)
- End users will also take part
- Each of these will keep the iTC 'on track'
- The PS and ES will also help
- Experience to date has also shown that vendors are much more mature than the myth would give them credit for! – Look at the CCUF

How you can take part

- Joining iTCs
  - Announcements will be made on the CC Portal
- Joining the CCUF
  - Link on final slide
- Using cPPs
  - Will be listed on the CC Portal – Increased end user involvement
- Reviewing and commenting

Summary

- CCRA is changing
- Supporting a more IT industry driven use of CC
- This should result in more effective and agile standards for IT products
- Better suited to the needs of Cyber defence
- There are many ways that you can get involved
- Come and join the work!
- Talk to us afterwards for more detail

Common Criteria

Useful Links

- www.commoncriteriaportal.org
  - Especially the first call for an iTC at www.commoncriteriaportal.org/communities/usb.cfm
- www.ccusersforum.org
- www.secureusballiance.org