Open CSIRT Foundation

Vote on adopting standardised TLP

Don Stikvoort
TF-CSIRT/TI Associate Member
Co-chair FIRST TLP SIG

Monday 15 May 2017

TLP background

- NISCC (UK) invented TLP (Traffic Light Protocol) around 2000
  - Purpose : encourage sharing of (sensitive) information
  - Sharing scope determined by colours WHITE, GREEN, AMBER and RED
- Picked up by govt teams first, later widely adopted
- TF-CSIRT/TI made support of TLP mandatory (MUST) in 2009
  - https://www.trusted-introducer.org/ISTLPv11.pdf
  - AMBER in this TLP version is based on the original NISCC intent where AMBER was meant for spreading to all relevant players who have a legitimate “need to know”
  - AMBER in some other versions (e.g. DHS) limits the spreading on a need-to-know basis *within the organisation* of the recipient only

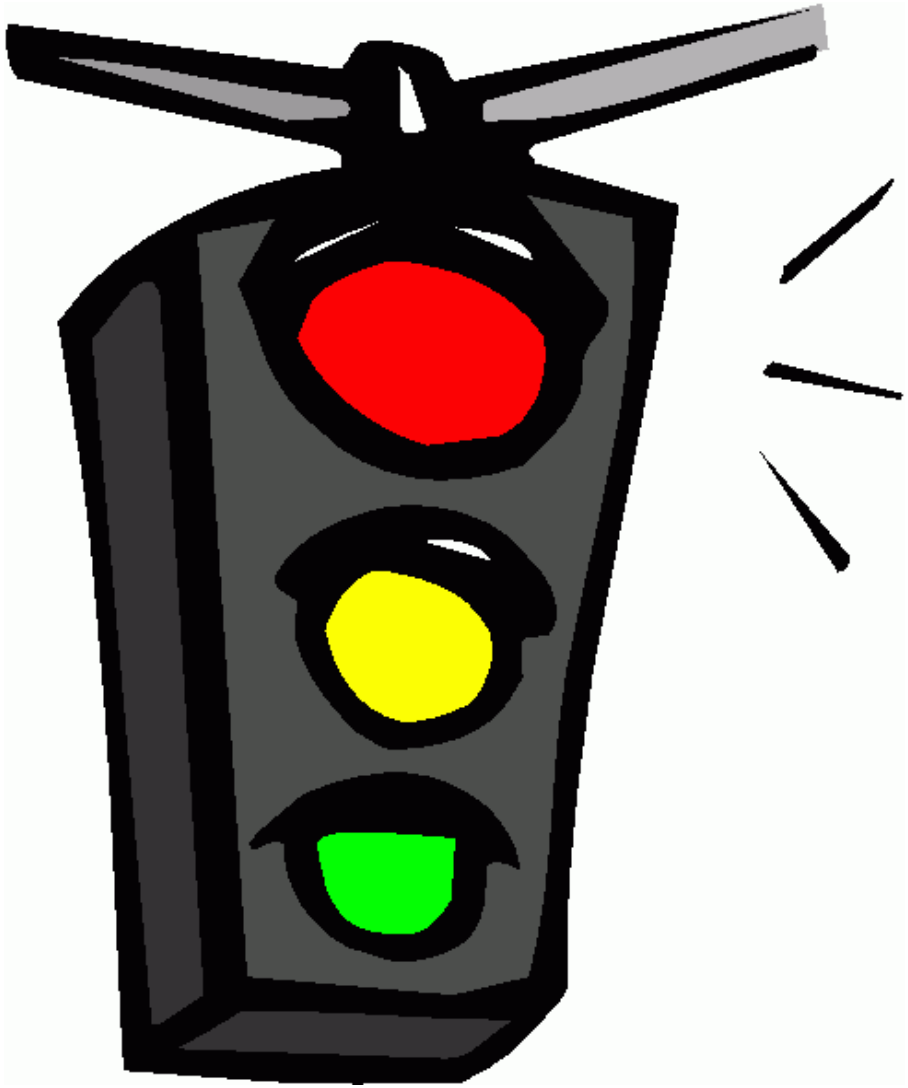

WARNING:
CONFUSION
AHEAD

TLP confusion

- And even more TLP versions leading to more confusion !
  - Some teams even used more than one version
- Discussed at FIRST conference in Berlin in 2015
- Installation of TLP SIG
  - Purpose: propose TLP standard for adoption by FIRST
  - Very diverse membership of CSIRTs, ISACs, APWG et al.
  - co-chairs Tom Millar (DHS) and Don Stikvoort (editor of TF-CSIRT/TI TLP version)
- Heated discussions
- SIG agreed on final text and proposed this to FIRST Board at conference in Seoul in 2016

An end to confusion ?

- Board accepted and published as FIRST Standard “TLP version 1.0”
  - https://first.org/tlp
- DHS, ENISA and others adopted TLP version 1.0
- Critique inside FIRST centered around TLP:AMBER scope
  - Led to lessons learnt, including better explanation of TLP
- TF-CSIRT discussed in September 2016 : “there was strong support from the meeting”
  - Difference with current TF-CSIRT/TI TLP version is small, as the AMBER definitions are similar



Vote proposal

- Keep TLP as MUST for Accreditation
- Replace current TLP by FIRST TLP version 1.0
- Migration between now and ?date?
- After ?date? all Accredited teams must support TLP version 1.0 and use it with peers
  - Internal use of both old **and** new TLP versions beyond ?date? is allowed but strongly discouraged

- ?date? = 1 October 2017 ?