The Standards People

Cybersecurity Act & Standardization

Presented by: **Luis Jorge Romero**

For: **ENISA-ESOs event, Brussels**

21.01.2019

February 2018: some requests put forward

Standards for Certification: clarify concepts and definitions

- ✓ the fundamental relationship between standards and certification to be explicitly described

Use the New Legislative Framework as a toolbox

- ✓ the text to include the clear sequence of *requirements – standards – certification*

Rethink levels of security under a "risk management" approach; redefine objectives

- ✓ a much higher level of objectives that avoid technical issues, left to standards to address

Ensure applicability and consistency with existing regimes

- ✓ e.g. TCAM and the Radio Equipment Directive 2014/53/EU, and the migration path from current national certification schemes

Specify governance and processes

January 2019: some good progress…

- Standards now recognized as the primary reference for a cybersecurity certification schemes
- Introduction of conformity self-assessment
- Assurance levels, now commensurate with the level of risk; assurance levels basic, substantial and high maintained but redefined
- Possibility to make a scheme mandatory after assessment; priority on sectors defined in annex II of NIS Directive; evaluation whether cybersecurity essential requirements for access to the internal market are necessary
- ESOs part of ENISA Advisory Group

… however

- New Legislative Framework NOT used
- Security objectives not made more high level
- More objectives added (applying to whole life cycle, do not contain known vulnerabilities, secure by default and by design, up-to-date SW/HW and mechanisms for secure updates)
- ESOs should be part of Stakeholder Cybersecurity Certification Group
- New Union rolling work programme of priorities for certification schemes; coordination with AUWP and ICT Rolling Plan?

From paper, to reality

- Define a good coordination scheme, ENISA-ESOs
- Define the role of standardization, i.e. how far should we standardize
- Ensure standardization in support of certification schemes
- Standardization being voluntary, how to ensure work on standards?
- Ensure Europe’s relevance in the Cybersecurity global space