DIGITALEUROPE

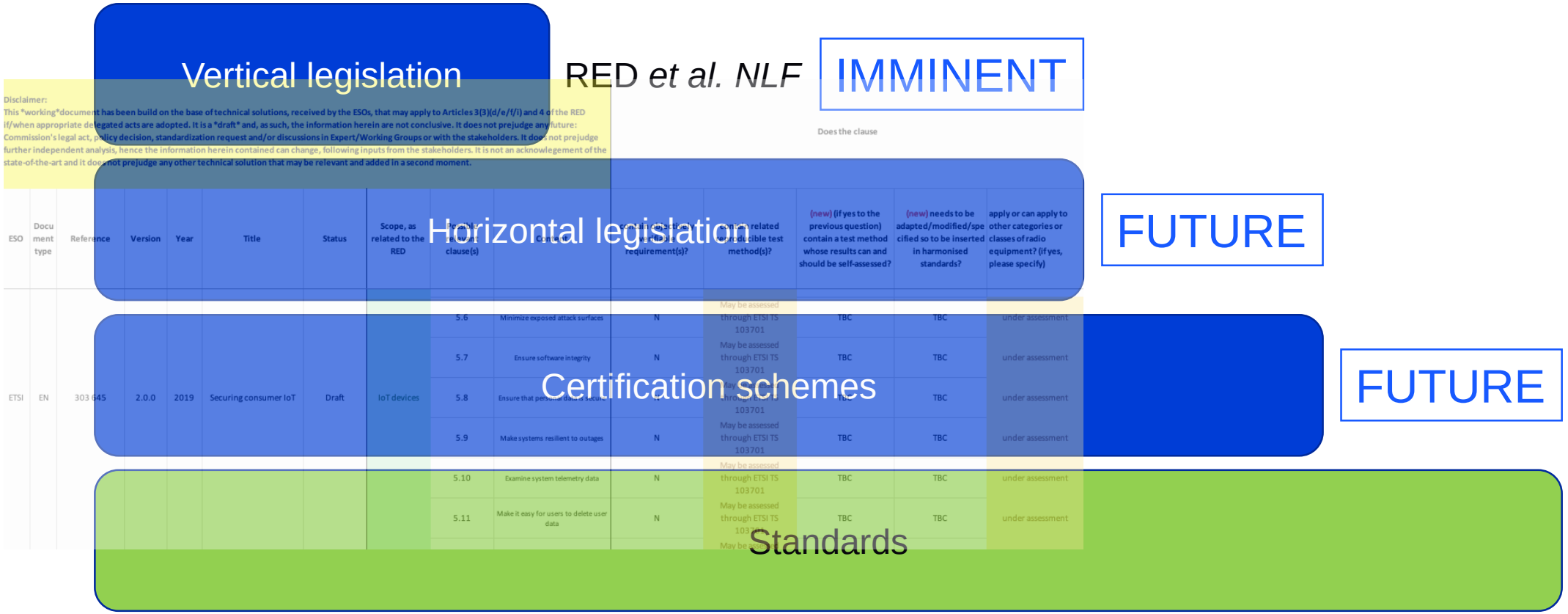
Cybersecurity Standardisation Conference 2021

Alberto Di Felice
Director for Infrastructure, Privacy and Security

Can’t wait for IoT security

DIGITALEUROPE

But mind the gaps – and the overlaps



Mapping the gaps

Source: European Commission, Study on the need of Cybersecurity requirements for ICT products, Workshop #1 – Problem Definition

DIGITALEUROPE

How does the RED perform?

Protection against accidental or unauthorised against storage, processing, access and disclosure	Protection against accidental or unauthorised d estruction, loss or alteration or lack of availability	Authorisation to access data and services	Identification of dependencies and vulnerabilities	Record of access
Art 3 - Essential requirements - Manufacturers	Art 3 - Essential requirements - Manufacturers	Art 3 - Essential requirements - Manufacturers	Not addressed	Not addressed
Verification of access	**Verification of the absence of vulnerabilities**	**Restauration of availability**	**Security by default and design**	**Secure update of software and hardware**
Not addressed	Not addressed	Not addressed	Not addressed	Not addressed

Fully addressed* Partially addressed Not addressed

** Requirements might be placed on the service provider*

Source: European Commission, Study on the need of Cybersecurity requirements for ICT products, Workshop #1 – Problem Definition

What industry needs

- Legal certainty and consistency – things standards can't take care of

  Measures to address IoT cybersecurity should aim to avoid multiple and diverging requirements

- Common baseline, with a differentiated approach to IoT per domain

  Cybersecurity requirements should always be based on risk and intended use – the higher the risk, the more stringent the requirements

- Standards must be ready before any legislation is implemented

  The development of appropriate IoT security standards and criteria should be allowed before enforcing or making applicable legislative measures

Thank you

DIGITALEUROPE