## Aim of the Workshop:

The aim of this workshop is to ensure a thorough understanding of the Legislative Guidance for Türkiye's Harmonization of the Regulation (EU) 2024/2847 on Horizontal Cybersecurity Requirements for Products with Digital Elements (Cyber Resilience Act) with all its aspects; with the ultimate objective of a smooth harmonization of this legislation and its effective implementation by Türkiye. The special relationship between Türkiye and the EU due to the Customs Union in effect will also be of critical importance for this workshop, as this framework will set the parameters of Türkiye's harmonization of this legislation. We aim to make sure that at the end of this workshop the participants will have acquired extensive knowledge about legislative requirements brought about by the Cyber Resilience Act, including the essential cybersecurity requirements for the design, development and production of products with digital elements; responsibilities of economic operators in relation to those products with respect to cybersecurity and market surveillance aspects among others. In this scope, especially considering Türkiye's leading position in the EU market as an exporter of white goods, and given the direct impact of the Regulation on product safety issues concerning the commercial activities of Turkish producers in the EU market, the aim is to ensure that participants acquire extensive knowledge about the CRA to prevent any negative impact on the free movement of goods between the Parties.

## Speakers:

- **XXX**
  [Ministry of Trade, Türkiye]
- **Mrs. Maria Vanessa UNTIEDT LECUONA**
  [xxx]
  Ministry of Justice, Kingdom of Spain
- **Mr. Enrico LABELLA**
  [xxx]
  Competition and Consumer Protection Authority, Italy
- **Mr. Danut MAFTEI, PhD**
  Senior Cyber Security Expert
  National Cyber Security Directorate - DNSC, Romania
- **Mr. Mihail George GURANDA**
  Former Superior Cyber Security Manager
  National Cyber Security Directorate - DNSC, Romania
- **Mr. Andrei Alexandru BABADAC**
  Trade Advisor
  Agency for Investment and Foreign Trade - AIFT, Romania

| **Day 1: 13-14 November 2025** | |
|---|---|
| **Chair: XXX, Ministry of Trade of Türkiye** | |
| Local time<br>*8:30 – 9:00* | *Registration, connecting participants, technical verifications* |
| **9:00 – 09:05** | **Welcome and introduction:**<br>• Ministry of Trade of Türkiye |
| **9:05 – 9:30** | – Legal Framework of the Customs Union between Türkiye and the European Union, Türkiye's legislative framework with specific emphasis on harmonization process of the CRA<br>**Speaker:** XXX, Ministry of Trade of Türkiye |
| **9:30 – 10:00** | **EU policies and legal framework on cyber issues**<br>– The Cyber Security Act (CSA). The EU cybersecurity certification frameworks / schemes for ICT products, ICT services and ICT processes<br>– The Cyber Resilience Act (CRA). Context, scope, essential requirements<br>– CRA: Obligations for manufacturers, importers, and distributors<br>– CRA: Risk-based approach to cybersecurity in products with digital elements<br>**Speaker**: Mr. Danut MAFTEI, Senior Cyber Security Expert, DNSC, Romania |
| **10:00 – 10:45** | **Challenges for SMEs and Manufacturers – Legal and Technical Readiness. The expected compliance burdens on SMEs and exporters from Türkiye entering the EU market**<br>– Documentation, technical file, and risk assessment requirements<br>– Cybersecurity governance for smaller manufacturers<br>– Training, certification, and capacity building needs<br>**Speaker:** Mr. Mihail George GURANDA, Former Superior Cyber Security Manager National, Romania |
| ***10:45 – 11:15*** | *Break* |
| **11:15 – 12:30** | **Conformity Assessment and Reporting Requirements**<br>– Technical documentation and compliance evidence<br>– Self-assessment vs. third-party evaluation under CRA<br>– Mandatory reporting: timelines and authorities involved<br>– Market surveillance methods and post-market obligations<br>**Case Study: CRA Compliance for White Goods Exported from Türkiye**<br>– End-to-end walkthrough of a compliance program<br>– Risk analysis, testing plan, documentation, and CE marking<br>– Exchange of best practices on the implementation of CRA<br>**Speaker:** Mrs. Maria Vanessa UNTIEDT LECUONA, position, Ministry of Justice, Kingdom of Spain |
| ***12:30 – 14:00*** | *Lunch break*<br>*Please be reminded to sign the attendance list* |
| **14:00 – 14:45** | **The Role of ENISA under the CRA**<br>– Coordination and support activities<br>– Vulnerability database and incident reporting<br>– Cooperation with national authorities<br>**The Responsibilities of National CERTs in the CRA Ecosystem**<br>– Incident response and vulnerability handling<br>– Collaboration with ENISA and cross-border coordination<br>– Manufacturer interactions and follow-up mechanisms<br>**Information Sharing with Non-EU Countries' CERTs with ENISA**<br>– Obligations of third-country manufacturers and notification process to ENISA<br>– Role of authorized representatives within the EU<br>– Channels for cross-border cybersecurity cooperation<br>**Speaker:** Mr. Enrico LABELLA, position, Competition and Consumer Protection Authority, Italy |
| ***14:45 – 15:15*** | *Break* |
| **15:15 – 16:00** | **Cybersecurity as a Market Standard: Turning EU Compliance into a Trade Advantage**<br>– **Badge-of-trust branding**: craft trade-promotion messages that market "CRA-ready" factories as the safest source for EU supply chains—mirroring Romania's own investor-outreach strategy<br>– **Service-layer booster**: highlight how CRA rules on secure updates and vulnerability reporting also back the free movement of digital services, giving Turkish exporters a dual-sector edge.<br>– **Risk-premium reducer**: connect CRA conformity certificates to OECD Investment Framework guidance, proving to financiers that Türkiye's manufacturers carry lower cyber–supply-chain risk<br>**Speaker**: Mr. Andrei Alexandru BABADAC, Trade Advisor, AIFT, Romania |
| **16:00 – 16:15** | AOB and wrap up of day 1 |

| **Day 2: 13-14 November 2025** | |
|---|---|
| **Chair: XXX, Ministry of Trade of Türkiye** | |
| Local time<br>***8:30 – 9:00*** | *Registration, connecting participants, technical verifications* |
| **9:00 – 10:00** | **Digital Product Trade Lanes: Harmonizing Standards for Competitive Exports**<br>– **Notified-body sprint team**: draw on Romania's multi-directive experience to help Türkiye accredit and monitor bodies that can certify CRA, Electromagnetic Compatibility Directive - EMC and Low-Voltage Directive - LVD requirements in one go<br>– **Mutual-recognition roadmap**: outline the legal steps for Turkish test reports to gain EU recognition (CRA, Art. 41), shaving weeks off time-to-market for smart appliances and IoT hardware<br>– **Standards convergence toolkit**: position ISO/IEC 27001 and ETSI EN 303 645 as dual-use benchmarks that satisfy CRA essentials while mirroring OECD digital-security principles<br>o Purpose and structure of the toolkit<br>o Role in supporting harmonized CRA compliance<br>o Overview of standardization efforts in progress<br>**CRA Alignment with EN 18031 Standards Series**<br>– EN 18031-1: Security Requirements for Digital Products<br>– EN 18031-2: Risk Assessment and Management Framework<br>– EN 18031-3: Vulnerability Handling and Disclosure Processes<br>– Using harmonized standards for presumption of conformity<br>**Speaker:** Mr. Andrei Alexandru BABADAC |
| **10:00 – 10:45** | **Alignment Roadmap and Regulatory Dialogue Mechanism. Co-developing a timeline and dialogue framework between TR and EU stakeholders for ongoing CRA implementation and regulatory updates**<br>– Milestones in the transition period (CRA enforcement dates and transitional measures)<br>– Participating in European cybersecurity certification schemes (e.g., EUCC)<br>– Continuous information exchange and mutual recognition of assessment procedures<br>**Speaker:** Mr Mihail George GURANDA |
| ***10:45 – 11:15*** | *Break* |
| **11:15 – 12:30** | **Interoperability of CRA and the RED Delegated Act (EU 2022/30)**<br>– Comparison of scopes and applicability<br>– Harmonized conformity assessment paths<br>– Timeline for parallel implementation<br>**Speaker:** Mr. Enrico LABELLA |
| ***12:30 – 14:00*** | *Lunch break*<br>*Please be reminded to sign the attendance list* |
| **14:00 – 14:45** | **Risks, threats, and vulnerabilities related to products and components with digital elements. Testing laboratories**<br>– Risks, threats, and vulnerabilities related to products and components with digital elements used by the governmental sector and Critical Information Infrastructure (CIIP)<br>– Security vulnerabilities identified in LTE and 5G technology that pose risks to citizens, businesses, state institutions, CIIP, and national security<br>– Testing laboratories for ICT products, ICT services and ICT processes<br>**Speaker:** Mr. Danut MAFTEI |
| ***14:45 – 15:15*** | *Break* |
| **15:15 – 16:00** | **Exchange of information on how the General Product Safety Regulation (GPSR) and Digital Services Act (DSA) regulation will enhance product safety, market surveillance, and inspection procedures in the context of cybersecurity requirements for products with digital elements.**<br>**Speaker:** Mrs. Maria Vanessa UNTIEDT LECUONA |
| **16:00 – 16:30** | AOB and wrap up of day 2<br>Closing remarks and end of the workshop |