DwyerOmega – EU Cyber Resilience Act: Obligation Statement

DWYEROMEGA™
Improving the world, one measurement at a time.

Thank you for contacting DwyerOmega regarding readiness for **EU Cyber Resilience Act (CRA)**.

We appreciate any proactive approach in preparing for the EU Cyber Resilience Act (CRA) and the collaborative way in which customers and suppliers are engaging.

DwyerOmega (including all its brands) acknowledges the importance of CRA compliance for continued commercialization of digital products in the EU and confirms our commitment to align with the regulation and support all our customers accordingly.

CRA Timeline Alignment
We are aligning with the regulatory milestones:

- **11 September 2026** – Readiness for vulnerability and incident reporting obligations
- **11 December 2027** – Full compliance with all applicable CRA requirements

We have initiated a structured internal program to ensure alignment with these timelines.

Current Status & Approach
We are currently progressing the following activities:

- **Product scoping and inventory** of all relevant products and services supplied to our customers and placed on the EU market.
- **Role and classification assessment** (manufacturer vs. component supplier - criticality categorization)
- **Initial gap assessment** against CRA Annex I requirements
- Initiation of CRA **Risk Assessments** and development of **Technical Documentation** (technical files) and implementation of **Secure by Design** practises across our global framework.

At this stage, our focus is on establishing a **robust and scalable compliance framework**, rather than issuing premature or incomplete artefacts.

Planned Deliverables
Our **phased response approach**, aligned with CRA timelines:
Near-term (2025 – early 2026):

- High-level product inventory and classification
- Initial gap assessment summary and remediation roadmap
- Confirmation of conformity approach (self-assessment vs. third-party)

By September 2026:

- Operational vulnerability and incident reporting processes aligned with CRA Article 14
- Defined communication and escalation procedures, including alignment with customer expectations where applicable

By December 2027:

- Full technical documentation (Annex VII)
- Complete user documentation (Annex II)
- EU Declaration of Conformity and CE marking, as applicable

Vulnerability & Incident Reporting
We are currently designing processes to ensure compliance with CRA reporting obligations by September 2026, including:

- Vulnerability monitoring and triage
- Incident detection and escalation
- External notification workflows

These processes are being developed in line with **CRA Article 14 (2), (3), and (4**) requirements, including:

- Early warning within 24 hours
- Follow-up notification within 72 hours
- Final reporting after mitigation

Standards & Framework Alignment
Our cybersecurity practices are being aligned with recognized industry standards, including IEC 62443 (where applicable), and we are assessing any requirements for third-party certification for relevant product categories.

Kind regards,

Jon Holland
Senior Technical Manager - Compliance
DwyerOmega