CROWDSTRIKE RESPONSE TO THE EUROPEAN COMMISSION CALL FOR EVIDENCE ON THE REVIEW OF THE DIGITAL DECADE POLICY PROGRAMME 2030

23 December 2025

I. INTRODUCTION

In response to the European Commission's ("Commission") Call for Evidence on the Review of the Digital Decade Policy Programme 2030 ("DDPP"), CrowdStrike offers the following views.

We approach these questions from the standpoint of a leading international, AI-native, cloud-native cybersecurity provider that defends globally distributed enterprises from globally distributed threats. CrowdStrike offers insights informed by multiple practice areas: cyber threat intelligence; proactive hunting, incident response and managed security services; and an AI-powered software-as-a-service cybersecurity platform and marketplace. Accordingly, this perspective is informed by CrowdStrike's role in protecting organizations from data breaches and a variety of other cyber threats.

II. COMMENTS

The DDPP has established a useful strategic and governance framework around four core pillars—skills, infrastructures, business digitalisation and digital public services—supported by common targets, national strategic roadmaps and multi-country projects. Whether the goal concerns gigabit connectivity, AI adoption by enterprises or digital public services, each depends on robust, modern cybersecurity capabilities. Threat activity against critical sectors continues to grow, and adversaries are moving faster and exploiting AI and cloud environments more aggressively.

CrowdStrike strongly supports this direction, particularly the explicit objectives to improve resilience to cyberattacks and to increase cybersecurity efforts across public and private organisations. Cybersecurity is a foundational enabler of every DDPP target. We commend the Commission for its 2025 analysis and recommendation for review of the DDPP. The DDPP's original targets pre-date the current wave of GenAI deployment and the review is the right moment to ensure that the programme recognises AI-enabled cybersecurity as a critical element of the digital ecosystem, and that it avoids regulatory disincentives to deploying best-in-class cybersecurity AI tools.

The DDPP sits alongside a broader EU agenda on data use. From a cybersecurity perspective, the main threat to European data is not lawful transfer but unlawful access by adversaries. Fragmented or overly restrictive data policies can reduce visibility for defenders, slow incident response and undermine the very security and sovereignty goals the Union seeks to advance.

In this context, CrowdStrike offers a set of concrete recommendations :

III. RECOMMENDATIONS

A. Refresh Digital Decade Targets and Indicators to Reflect Cybersecurity, AI and Resilience

CrowdStrike supports retaining the DDPP's four headline target areas. They provide a clear and communicable structure for the decade. However, we recommend that the review:

1. **Explicitly elevate cybersecurity as a cross-cutting dimension in each target cluster.**
   Article 3 of the DDPP already refers to improving resilience to cyberattacks and achieving at least basic levels of cybersecurity across public and private organisations. This should be operationalised by:

   - Linking the "secure, resilient and sustainable infrastructures" target directly to adoption of modern security architectures (e.g. Zero Trust, managed detection and response, cloud-native protection) and to the deployment of multi-country security operations centres (SOCs) already identified in the DDPP annex.
   - Integrating concrete cybersecurity sub-indicators into the business and public-sector digitalisation targets (for example, coverage of endpoint detection and response (EDR), next-generation SIEM, identity threat protection and continuous threat-hunting activities in critical and high-risk sectors).

2. **Ensure that AI-enabled cybersecurity is recognised and not inadvertently disincentivised.**
   In line with the AI Act discussions, AI systems deployed solely for cybersecurity purposes should not face disproportionate burdens that would discourage their use, especially in critical infrastructure. The DDPP review can highlight

AI-enabled defense as a necessary ingredient for achieving the 2030 targets in a threat environment where adversaries also operate "at machine speed."

Overall, we recommend keeping the four pillar structure and existing high-level targets, while reinforcing and updating them through cybersecurity- and AI-specific sub-targets and indicators.

B. Accelerate Progress Through Practical Cybersecurity Adoption Levers

Digital transformation cannot be accelerated if organisations lack the means to defend the resulting infrastructures and data. CrowdStrike recommends that the review highlight measures that Member States can embed in their national Digital Decade strategic roadmaps:

1. **Promote state-of-the-art security practices and technologies.**
   Effective cybersecurity depends on risk-based architectures that leverage cloud security, EDR, next-generation SIEM, AI-based prevention and identity threat detection and response. Embedding such practices in DDPP implementation guidance—especially for SMEs and public authorities—would directly support faster, safer progress towards all digital targets.

2. **Support managed security services and 24/7 monitoring.**
   Many entities do not have the scale or maturity to operate a round-the-clock SOC. Reliance on qualified managed security service providers can substantially improve security outcomes and free internal resources for domain-specific work. The DDPP review could encourage Member States to use EU funds and national instruments (including the next MFF and possible "cybersecurity vouchers") to facilitate access to such services for SMEs, healthcare providers and local authorities.

These measures would allow the DDPP to move from technology-only uptake metrics to a more integrated view of secure digital acceleration.

C. Streamline Governance and Reduce Administrative Burden While Maintaining Coherence

The DDPP has introduced a structured cooperation mechanism, including national roadmaps, annual reporting and joint commitments. At the same time, the broader EU digital and cybersecurity regulation map has become denser—NIS2, the Cyber

Resilience Act, DORA, the Cybersecurity Act, the AI Act and forthcoming "Digital Omnibus" measures all impose planning and reporting requirements.

To reduce administrative burden while preserving effectiveness, CrowdStrike recommends that the review:

1. **Align DDPP reporting with existing sectoral obligations.**
   Where possible, DDPP monitoring should re-use information already produced under NIS2, DORA, CRA or sectoral frameworks, rather than creating parallel templates. For example, incident and risk assessment data collected under NIS2 could feed DDPP indicators on resilience, avoiding duplicative reporting.

2. **Focus governance on outcomes and risk, not exhaustive checklists.**
   Security should be measured by outcomes and real-world risk, not by rigid, one-size-fits-all compliance lists. The DDPP review could similarly encourage Member States to concentrate on demonstrating progress against security-related targets rather than on expanding formal reporting.

3. **Provide clearer guidance on the interaction of DDPP with other frameworks.**
   The Commission could issue a concise mapping note showing how DDPP objectives and indicators relate to key horizontal and sectoral instruments (NIS2, CRA, AI Act, Data Union Strategy, etc.). This would help national administrations design coherent roadmaps and reduce fragmentation risks that can themselves undermine cybersecurity.

In our view, a streamlined, outcome-oriented governance model will make the DDPP more attractive to Member States and stakeholders and help sustain political focus beyond 2030.

D. Align DDPP with Sustainable Financing for Cybersecurity and Data Infrastructure

The Call for Evidence emphasises that much of the EUR 288.6 billion mobilised to date depends on the Recovery and Resilience Facility, which will end in 2026, and that structural obstacles impede financing of the EU's digital transformation. From a cybersecurity standpoint, we suggest that the review:

1. **Use the DDPP to signal long-term priorities for digital and cybersecurity investment.**
   The review report can inform the design of the next Multiannual Financial Framework, the European Competitiveness Fund and National and Regional

Partnership Plans. It should highlight that investments in secure cloud infrastructure, AI-enabled cyber defense, multi-country SOCs, and cybersecurity skills are core enablers of DDPP targets and should be treated as strategic priorities.

2. **Facilitate access to finance for SMEs and high-impact sectors.**
   As highlighted in the healthcare cybersecurity context, targeted financial instruments (including vouchers or dedicated calls) can help resource-constrained entities adopt external cybersecurity services and modern security tooling. The DDPP review could encourage inclusion of such instruments in future EU programmes and national co-financing schemes linked to DDPP objectives.

By explicitly linking digital-transformation funding to concrete, risk-based cybersecurity investments, the DDPP can help ensure that Europe's digital growth is sustainable and secure.

IV. CONCLUSION

CrowdStrike supports the Commission's decision to review the Digital Decade Policy Programme at this pivotal moment. The DDPP has already provided an important common framework for Europe's digital ambitions. The review is an opportunity to ensure that the programme remains aligned with fast-moving technological, geopolitical and cyber-threat developments, including the transformative impact of AI.

If designed and implemented with the above listed recommendations in mind, the reviewed DDPP can significantly strengthen Europe's competitiveness, sustainability and security, and ensure that the Digital Decade is also a decade of enhanced cyber resilience. CrowdStrike stands ready to support the Commission's efforts by sharing technical expertise, global threat intelligence, and best practices in the secure digitisation of our infrastructure, public services and businesses.

V. ABOUT CROWDSTRIKE

CrowdStrike (Nasdaq: CRWD), a global cybersecurity leader, has redefined modern security with one of the world's most advanced cloud-native platforms for protecting critical areas of enterprise risk – endpoints and cloud workloads, identity and data.

Powered by the CrowdStrike Security Cloud and world-class AI, the CrowdStrike Falcon® platform leverages real-time indicators of attack, threat intelligence, evolving adversary tradecraft and enriched telemetry from across the enterprise to deliver hyper-accurate detections, automated protection and remediation, elite threat hunting and prioritized observability of vulnerabilities.

Purpose-built in the cloud with a single lightweight-agent architecture, the Falcon platform delivers rapid and scalable deployment, superior protection and performance, reduced complexity and immediate time-to-value.

CrowdStrike: We stop breaches.

Learn more: https://www.crowdstrike.com/.

CONTACT

We would welcome the opportunity to discuss these matters in more detail. Public policy inquiries should be made to:

Drew Bagley
VP & Counsel, Privacy and Cyber Policy

Līga Rozentāle, CISM
Director, Public Policy EU/International

Email: policy@crowdstrike.com

###