

POSITION | DIGITAL POLICY | CYBERSECURITY AND AI

Action Plan on Cybersecurity and Artificial Intelligence

*Evaluation of the European Commission's Communication***21 September 2026**

German industry welcomes the European Commission's Action Plan on Cybersecurity and Artificial Intelligence as a necessary response to the growing impact of AI on the cyber threat landscape. The Action Plan correctly recognises AI as both an opportunity for strengthening cyber resilience through improved detection, vulnerability management, incident response, and a driver of more automated, scalable and targeted cyberattacks. Its focus on secure testing environments, evaluation capacity, vulnerability management, sovereign compute, innovation and skills addresses key challenges for Europe. However, the Action Plan remains too vague on implementation, access to the latest models, financing, liability and the participation of Small and Medium Enterprises (SMEs).

German industry's core recommendations

1. The Action Plan must not become a basis for additional regulatory layers on top of the Artificial Intelligence Act (AI Act), the Cyber Resilience Act (CRA), the Cybersecurity Act (CSA), the Directive on Measures for a High Common Level of Cybersecurity across the Union (NIS 2 Directive) and the Digital Operational Resilience Act (DORA). As these instruments already provide the legal framework for cybersecurity in the age of artificial intelligence, the European Commission together with the EU Member States should focus on implementation, investment, testing, skills development and the pooling of expertise rather than additional regulation. The key challenge is therefore not to close regulatory gaps but to ensure that the existing frameworks are properly aligned and coordinated and that the relevant institutions have the expertise, resources and capabilities to keep pace with the scale, speed and complexity of AI-enabled risks.
2. A strong European network of Artificial Intelligence Safety and Security Institutes (AISIs) can play an important role in this regard. National institutes should be coordinated at the European level to ensure cooperation, specialisation and the exchange of expertise across Europe. The planned German AISI should become a leading centre of technical excellence that is well-funded, internationally connected and clearly non-regulatory. It should remain an agile institution focused on independent expertise, cutting-edge research and the strengthening of AI intelligence security capabilities, rather than evolving into an additional regulatory authority.
3. While the Commission's Action Plan provides a solid foundation for enhancing cybersecurity and supporting AI adoption in Europe, it does not sufficiently address the international regulatory environment in which European companies operate. The EU should therefore complement the Action Plan with a fourth pillar dedicated to the mutual recognition of cybersecurity standards, helping to reduce fragmentation while maintaining a high level of cybersecurity protection.

The Action Plan will be judged by its ability to strengthen innovation, competitiveness and operational resilience in practice. For German industry, this requires less bureaucracy, stronger stakeholder involvement and a clear commitment to building European and German technological capabilities.

Bundesverband der Deutschen Industrie e.V. / Federation of German Industries

EU Transparency Register: 1771817758-48 | German Lobbyregister: R000534

Lukas Kahler and Steven Heckler | Innovation, Security and Technology

Table of Content

Pillar 1: Making frontier AI safe, accessible and deployable for European cybersecurity	3
1.1 EU Evaluation capacity for AI models	3
1.2 The Blueprint	3
1.3 Secure Testing Environment	4
Pillar 2: Preparing the EU's cyber ecosystem for the age of AI	4
2.1 Guidance and best practices against AI-powered threats	4
2.2 Vulnerability management fit for the AI age	5
2.3 Open Source Resilience Campaign	5
Pillar 3: Scaling European AI capabilities for cyber	6
3.1 The EU Grand Challenge	6
3.2 Building European frontier capabilities	6
3.3 Boosting cybersecurity skills for the age of AI	7
Pillar 4: EU-US Mutual Recognition of cybersecurity standards	7
4.1 Fragmentation of cybersecurity standards	7
4.2 Proposed solution: Mutual recognition agreement.....	8
4.3 Principles of a cybersecurity mutual recognition agreement.....	8
Necessity of the German AISI	9
Imprint	10

Pillar 1: Making frontier AI safe, accessible and deployable for European cybersecurity

The Commission's first pillar addresses one of the great strategic questions for Europe: how can advanced and frontier AI capabilities be made available promptly for legitimate cybersecurity purposes without creating the risk of misuse. German industry supports the view that the Union needs stronger capacity to evaluate, access and test AI models with cyber capabilities. At present, access to such capabilities is often shaped by non-European providers and opaque access decisions. This creates risks for European sovereignty and for the ability of companies and public authorities to respond quickly to threats.

1.1 EU Evaluation capacity for AI models

The European Commission plans to support the establishment of an EU capacity for evaluating AI models in the field of cybersecurity by 2027. This capacity should support Member States' emerging evaluation ecosystems, assist the AI Office's regulatory work and assess model capabilities and mitigation measures. German industry stresses the importance of national Artificial Intelligence Security Institutes. The EU evaluation capacity should be established as an integrated framework that combines EU-level coordination with top-notch national expertise. It is paramount that national AISIs cooperate closely with each other and do not merely duplicate each other's work. This role should be integrated into the mandate of the institutes. ENISA is well placed to serve as the EU's point of coordination for AI security, given its technical expertise and its coordination role across the cybersecurity ecosystem; the ongoing review of the Cybersecurity Act provides an opportunity to equip it with the mandate and resources required to support this task. National AISIs should provide independent, science-driven technical expertise, including the development of evaluation methodologies, frontier model evaluations and red-teaming. The AI Office is already developing methodologies and benchmarks for systemic risks under the general-purpose AI (GPAI) framework and should work closely with the network of national AISIs to advance evaluation science. Where companies already comply with recognised international standards and established evaluation frameworks, these should be taken into account within the regulatory process. Such standards could be recognised through a rebuttable presumption of conformity, providing legal certainty, incentivising best practices and avoiding duplicative compliance efforts.

1.2 The Blueprint

The planned European Blueprint for structured access to advanced AI capabilities, to be developed by the Commission in coordination with ENISA by Q4 2026, is one of the most important measures in the plan. The Commission intends for the Blueprint to define criteria for granting access to advanced models, identify eligible organisations, include security criteria, streamline access and provide contingency measures if access is restricted or withdrawn.

German industry welcomes this approach, as European cybersecurity providers, industrial companies and operators of critical infrastructure urgently need access to advanced AI capabilities to strengthen their resilience. The Blueprint should also explicitly include European manufacturers whose products, components and systems are used in critical infrastructure, as they are an integral part of the value chain and need access to strengthen resilience at the source. However, the Blueprint must not become an additional bureaucratic permission system or hinder the mutual exchange of information and knowledge between Member States and like-minded partners. It has to enable access, not delay or even prohibit it because of unrealistic thresholds. The Commission's assurance that the Blueprint will not introduce new obligations for providers is of utmost importance and should be kept up constantly.

The Blueprint should include clear eligibility criteria, simple digital application procedures, defined decision periods, confidentiality rules and fast-track access for trusted European cybersecurity providers, critical infrastructure operators and key European manufacturers in critical infrastructure value chains.

1.3 Secure Testing Environment

The plan proposes that ENISA, the Joint Research Centre of the European Commission and other European services develop a secure testing platform for artificial intelligence with advanced cyber capabilities by Q4 2026. Such a platform should allow testing of AI in cybersecurity use cases such as vulnerability scanning, remediation and incident response. Secure testing environments should explicitly include telecommunications networks, 5G and 6G infrastructures, edge and cloud environments, and autonomous network operations. Testing should cover cross-domain agent interaction, fail-safe operation, human override, rollback mechanisms and the secure execution of AI-initiated changes in critical network infrastructures. The Action Plan also highlights the use of cyber ranges, meaning controlled environments that simulate real systems without endangering actual infrastructure. Already existing cyber ranges will be adapted and expanded and only in special circumstances newly one's will be opened. Participating industry actors could gain access to insights derived from testing, which may help inform their development and deployment of advanced cyber capabilities.

German industry supports the secure testing environments and the chosen way of implementing them. At the same time, the Action Plan underestimates the conditions under which industries will be able to contribute. To ensure know-how protection, companies should not be expected to provide environments, data, operational know-how or sector-specific expertise without robust safeguards. Trade secrets, sensitive security information, intellectual property and liability questions must be clarified in advance. SMEs that for various reasons cannot contribute should also receive subsidised or shared access, otherwise the measure risks becoming only relevant for large actors.

Pillar 2: Preparing the EU's cyber ecosystem for the age of AI

The second pillar addresses Europe's preparedness for AI-powered cyber threats. German industry agrees that cybersecurity requirements, vulnerability management and open-source resilience are becoming increasingly important. However, the Commission's proposals must be realistic from an international perspective. Companies are already facing significant implementation pressure from the NIS 2 Directive, the Cyber Resilience Act, DORA, the EECC, the DNA (draft) and the AI Act. Additional regulatory requirements, even if framed as guidance or best practices, could create de facto compliance pressure. The Action Plan should simplify requirements by streamlining them and ensure a coherent regulatory framework that prevents duplicative conformity assessments and eliminates contradictory compliance obligations. For companies operating across several Member States, cybersecurity obligations should allow for the centralised fulfilment of registration, documentation and reporting. Such an intra-group privilege would reduce duplication, improve consistency and enable more effective incident handling without weakening supervisory access to relevant information. The objective should be to make the existing cybersecurity frameworks AI-ready rather than to create a parallel AI security regime. This should also apply in public procurement. If guidance, best practices or voluntary certifications were transformed into mandatory eligibility criteria, voluntary instruments would create new market barriers.

2.1 Guidance and best practices against AI-powered threats

ENISA is expected to issue guidance, recommendations, advisories and best practices on protection against AI-powered threats and on the secure integration of AI into cybersecurity operations from Q3 2026 onwards. It is welcome that the Commission explicitly states that SMEs are to be taken into account as it is them who often are especially vulnerable to such threats.

Still, guidance must remain non-binding in practice as well as in form. There is a risk that ENISA guidance could become quasi-regulation if supervisors, auditors, customers or public procurers treat it as mandatory. This would create unwanted additional obligations without a proper legislative process. ENISA guidance should, therefore, be concise and include sector-specific examples, SME-oriented templates and realistic implementation pathways. Guidance must clearly distinguish between legally binding requirements and voluntary good practices. The secure operation of AI agents requires security controls and permissions to be bound to the approved task and its risk. Each agent should have a registered and verifiable identity and receive only the minimum permissions required for its task. Zero Trust principles should ensure continuous verification of the agent's identity, task integrity, runtime context and communications. Compromise, impersonation or unauthorised task changes must result in immediate restriction or revocation, while critical actions should require human approval. Interoperable and machine-readable security, privacy and compliance attestations should enable trusted agent-to-agent cooperation across companies and Member States.

2.2 Vulnerability management fit for the AI age

The European Commission correctly stresses that AI will accelerate vulnerability discovery and that European actors must improve their ability to analyse, prioritise and remediate vulnerabilities before they are exploited at scale. AI-driven vulnerability discovery represents a structural shift in cybersecurity. The European Commission should support the development of a European vulnerability management strategy that strengthens ENISA, the national CSIRTs, the EU Vulnerability Database and coordinated disclosure frameworks, enabling validation, prioritisation and remediation to keep pace with machine-speed threats.

The EU Vulnerability Database, the CRA Single Reporting Platform, national databases and global vulnerability systems must be interoperable. This interoperability can strengthen situational awareness and help identify systemic and supply chain vulnerabilities across the EU. Vulnerability management should cover the entire AI supply chain, including models, datasets, fine-tuning components, retrieval sources, agent tools, interfaces, orchestration layers and supporting software. Standardised and machine-readable component inventories and provenance information should enable organisations to identify affected dependencies, assess their exposure and implement updates or mitigation measures rapidly. Reporting obligations should be streamlined and not duplicated. SMEs need practical tools and managed support, not additional reporting complexity.

Industrial Operational Technology (OT) environments require specific attention throughout the implementation of the Action Plan. While artificial intelligence may significantly accelerate vulnerability discovery, remediation in industrial environments is often constrained by operational, safety and regulatory requirements. Production systems, process control environments and safety-related systems cannot be patched, modified or restarted at the same pace as conventional IT systems. The Commission should therefore ensure that AI-driven vulnerability management and remediation initiatives explicitly take account of the specific characteristics of OT and Industrial Control Systems (ICS). Secure testing environments and cyber ranges should include representative industrial infrastructures, including process control systems, industrial networks and safety-critical environments. In addition, AI-powered cybersecurity solutions should be developed and validated using realistic industrial use cases and datasets in close cooperation with operators of industrial facilities. Strengthening cyber resilience in Europe's critical industrial infrastructure requires a balance between cybersecurity objectives with operational safety, reliability, business continuity and regulatory compliance.

2.3 Open Source Resilience Campaign

The European Commission, Member States, open-source communities, Union entities and industry will launch the first Open Source Resilience Campaign in Q4 2026. The Action Plan rightly notes that open-source software is deeply embedded in critical infrastructure and that vulnerabilities in

components can create systemic risks. The Open Source Resilience Campaign must extend beyond traditional software to free and open-source AI components, in particular AI models and general-purpose AI models, model weights, evaluation tools and, where legally possible, relevant datasets. Open models developed in Europe for cybersecurity should be treated as strategic resilience assets and supported through sovereign compute capacity, independent security evaluations, transparent documentation, vulnerability management and sustainable long-term maintenance.

This would reduce critical dependencies on non-European providers and ensure that European companies and public authorities retain reliable access to models that can be independently evaluated, adapted and operated under European control and in line with Union law and European values. Open-source status alone must not be considered evidence of security or legal compliance. The proposed voluntary sponsorship scheme and catalogue of AI-powered patching and remediation services are useful ideas.

Pillar 3: Scaling European AI capabilities for cyber

Third, German industry strongly supports the European Commission's recognition that Europe must not only regulate AI and cybersecurity but also build and scale its own AI-powered cybersecurity solutions. By competing at the highest level, the European Union can shape the way Frontier AI is being used on an international scale. However, the Action Plan remains too vague on how European companies, especially start-ups, scale-ups and SMEs, will gain access to compute capacity, funding, testing environments and customers.

3.1 The EU Grand Challenge

The European Commission, supported by the European Cybersecurity Competence Centre and in cooperation with ENISA, will launch an EU Grand Challenge on AI-assisted vulnerability remediation in Q4 2026. The Commission correctly notes that AI-assisted vulnerability discovery is advancing faster than AI-assisted remediation, creating an advantage for attackers.

German industry welcomes this focus, as remediation is one of the most urgent operational bottlenecks. However, the Grand Challenge must not become another complex EU funding exercise dominated by organisations with large administrative departments. If the procedure is too burdensome, start-ups, SMEs and specialised cybersecurity providers may not participate. Graduated timelines and advisory support, rather than premature enforcement, have proven effective for SME compliance in comparable frameworks, and should guide the Grand Challenge's SME provisions as well.

The Grand Challenge should therefore be deployment-oriented and accessible. Application procedures should be simple, digital and predictable. Selection criteria should focus on technical quality, operational relevance and potential for market deployment. Intellectual property rights and business secrets must be protected. Industrial users should be involved to ensure that solutions work in real environments, including operational technology and safety-critical systems.

European cyber resilience requires more than sovereign computing capacity. European companies and critical infrastructure operators must have reliable access to trusted AI models for cybersecurity that are developed and operated under European control, subject to predictable licensing conditions and without unilateral dependencies on non-European infrastructure or access decisions.

3.2 Building European frontier capabilities

Together with the Member States, the European Commission aims to make the compute capacity of AI Factories available for testing, training and deploying advanced and frontier AI models for cyber

resilience on sovereign compute. The Action Plan links this to wider ambitions around AI Factories, Gigafactories, secure data-sharing mechanisms and AI-ready datasets.

German industry supports access to sovereign computing facilities. Without sufficient compute capacity, European cybersecurity providers will struggle to compete with non-European providers. However, the Action Plan does not sufficiently explain how companies will access this capacity in practice. Companies need transparent access criteria, predictable pricing, secure handling of sensitive industrial data, clear IP rules and simple application procedures. SMEs should receive dedicated access opportunities, not merely theoretical eligibility. Regarding frontier AI security testing, the planned German AISI should be connected to AI Factory access and evaluation processes.

3.3 Boosting cybersecurity skills for the age of AI

The European Commission will work with Member States and industry through the Cybersecurity Skills Academy to develop training modules for cybersecurity professionals on the use of AI for cybersecurity by Q4 2026. ENISA is also expected to update the European Cybersecurity Skills Framework to include AI-related competencies.

German industry welcomes the Academy and recommends that its training cover a broad range of skills beyond technical AI use, including the supervision of AI outputs, the handling of sensitive data, the recognition of model misuse and an understanding of risks such as prompt injection, adversarial attacks and data poisoning. SMEs need affordable, modular and directly applicable formats. The Commission should avoid creating training schemes that look strong on paper but are too detached from business practice. Building Europe's AI safety and cybersecurity capacity will also require close cooperation between governments, industry, academia and research institutions. The Commission and Member States should work with industry to support specialised training programmes, joint research initiatives, skills partnerships, fellowships and talent exchanges, drawing on the expertise, tools and practical experience that industry already possesses.

Pillar 4: EU-US Mutual Recognition of cybersecurity standards

4.1 Fragmentation of cybersecurity standards

While the Commission's Action Plan provides a solid foundation for enhancing cybersecurity and supporting AI adoption in Europe, it does not sufficiently address the international regulatory environment in which European companies operate. For internationally active businesses, the ability to scale technologies, security processes and compliance frameworks across jurisdictions increasingly depends on greater alignment and interoperability of cybersecurity requirements. The EU should therefore complement the Action Plan with a fourth pillar dedicated to the mutual recognition of cybersecurity standards, helping to reduce fragmentation while maintaining a high level of cybersecurity protection.

There is growing international recognition that the global fragmentation of cybersecurity regulatory frameworks poses a strategic challenge. According to a 2024 report by the Office of the U.S. National Cyber Director, Chief Information Security Officers (CISOs) reported spending between 30-50% of their time on regulatory compliance activities across multiple regulatory regimes and jurisdictions, diverting resources away from combatting cyber threats¹.

The growing regulatory fragmentation is undermining companies' cyber defense operations, preventing the implementation of consistent security measures across different jurisdictions, and adding

¹ See ONCD report [here](#).

complexity to time-sensitive incident response activities. In addition, the lack of global alignment on cybersecurity regulations is also creating barriers to cross-border trade and technology adoption. The 2025 World Trade Organization and International Chamber of Commerce (WTO-ICC) business survey found that firms of all sizes, income levels and sectors now identify the regulatory uncertainty around cybersecurity as a key obstacle to AI adoption across borders². The WTO has also found that cybersecurity regulations have become a major source of concern raised by WTO members in the Council for Trade in Services, and that cybersecurity-related measures have been increasingly reported by members under the Agreement on Technical Barriers to Trade³.

The OECD *Towards international coherence of cybersecurity regulations* report (2026)⁴ identified a number of key drivers of this fragmentation. These include differing threat perceptions, sector-specific legacy frameworks, asynchronous policy development and the multiplicity of regulatory actors with overlapping mandates. The OECD is seeking to address these drivers by refocusing its workplan on cybersecurity cooperation – including developing common principles for regulation, harmonising incident reporting requirements and building a common cybersecurity taxonomy. In parallel, policymakers are beginning to incorporate regulatory alignment and interoperability objectives into cybersecurity policy and regulatory reform efforts.

4.2 Proposed solution: Mutual recognition agreement

Regulatory simplification efforts in the EU, the United States and other jurisdictions are important first steps but they cannot eliminate duplication across borders. Together, these initiatives create a timely opportunity to advance international regulatory alignment. The 2026 U.S. National Cyber Strategy prioritises streamlining cybersecurity regulation, while the EU's Digital Omnibus and Cybersecurity Act 2 aim at reducing overlapping requirements and improve interoperability.

The 2025 EU-US Framework on an Agreement on Reciprocal, Fair and Balanced Trade already established a political commitment to negotiate a cybersecurity Mutual Recognition Agreement. The next step is now to define its wider scope and ambition. The MRA should go beyond a narrow technical arrangement limited to specific conformity assessments and notified bodies. Product-level mutual recognition can provide a practical starting point, but the greater opportunity lies in creating a comprehensive framework for the recognition of equivalent, trust-based cybersecurity requirements. The Commission's ongoing Digital Omnibus and Digital Fitness Check provide a clear policy window for advancing this broader approach.

The EU and the United States should seize this auspicious moment to shape and also create common interoperable cybersecurity requirements before divergent rules become entrenched in legal frameworks that cannot keep pace with evolving threats, technologies and markets.

4.3 Principles of a cybersecurity mutual recognition agreement

An EU-U.S. cybersecurity mutual recognition agreement (MRA) should achieve the following overarching goals:

- **Adherence to internationally recognised cybersecurity and resilience standards:** Compliance with internationally recognised standards, including ISO 27001 and the NIST

² See WTO report [here](#).

³ Ibid.

⁴ See OECD report [here](#).

Cybersecurity Framework, should be accepted as a valid basis for satisfying compliance requirements under both frameworks.

- **Supply chain security alignment:** EU-US alignment on approaches to supply chain security based on objective, risk-based criteria.
- **Mutual recognition of public sector certification schemes:** Providers certified under schemes used for public procurement should be able to rely on mutual recognition to access procurement markets on both sides of the Atlantic.
- **Convergence of security approaches and requirements:** Common approaches to risk management, vulnerability coordination, and Software Bills of Materials (SBOMs) should be adopted to reduce compliance divergence and support interoperable security practices.
- **Procedural harmonisation:** Incident reporting timelines, definitions, and thresholds should be aligned across both jurisdictions, building on the EU-U.S. Cyber Dialogue to enable a coherent and timely cross-border response.
- **Recognition of conformity assessments:** Conformity assessments conducted by accredited third-party laboratories in one jurisdiction should be accepted as valid in the other, eliminating redundant testing requirements. This level of recognition should, however, complement rather than substitute for deeper equivalence-based recognition of the underlying standards themselves.
- **Recognition of third-party audits:** Audits and certifications performed under one jurisdiction's framework should satisfy equivalent requirements in the other, eliminating duplicative compliance exercises for providers operating across both markets.

Necessity of the German AISI

In line with the European Commission's vision, Germany has already taken the first steps towards establishing a national AISI, including through a strategic partnership with its counterpart in the United Kingdom. It is a matter of utmost importance for Germany's and Europe's technological sovereignty, security and industrial competitiveness that this institute is capable of competing at the highest international level.

Frontier AI models are increasingly affecting cybersecurity, critical infrastructure, public administration and industrial value chains. Germany therefore needs a dedicated technical institution capable of evaluating advanced AI models, assessing their cyber capabilities and providing reliable situational awareness. Currently, Germany is at a crossroads, deciding whether to develop a leading institution akin to its already well-established counterpart in the United Kingdom or an ordinary grey mouse agency condemned to a Sisyphean struggle to keep pace with the rapidly evolving realities of artificial intelligence.

The European Commission envisions strong cooperation among national AI Safety and Security Institutes. It should also set out a clear roadmap for aligning existing and future national AISIs with the EU framework from the outset. To maximise their effectiveness, it must preserve the fast-paced and agile nature of these institutes, which is essential to their mission. Their capabilities should not be undermined by excessive regulation or administrative burdens. This cooperation should also extend beyond the EU. Given the global nature of frontier AI development and cyber threats, the EU and its Member States should engage with international initiatives to advance shared evaluation methodologies and interoperable approaches to AI safety and security. Such cooperation should extend beyond joint testing to include common risk taxonomies, safety frameworks, transparency practices and technical standards.

Imprint

Bundesverband der Deutschen Industrie e.V. (BDI) / Federation of German Industries
Breite Straße 29, 10178 Berlin
www.bdi.eu
T: +49 30 2028-0

EU Transparency Register: 1771817758-48

German Lobbyregister: R000534

Editors

Lukas Kahler
Intern
Innovation, Security and Technology
T: +49 30 2028-1461
l.kahler@bdi.eu

Steven Heckler
Senior Expert Cybersecurity and Digital Business Identities
Innovation, Security and Technology
T: +49 30 2028-1523
s.heckler@bdi.eu

Document number: D 2336