22 June 2026

A practical path to EU-US cybersecurity mutual recognition

Executive summary

The August 2025 EU-US trade framework created a clear and time-sensitive political commitment: the EU and the US committed to negotiating a cybersecurity mutual recognition agreement. The immediate priority is to turn that commitment into an implementable first tranche, because the issue sits at the intersection of wider EU-US discussions on trade and the establishment of the EU-US Digital Dialogue.

The cyber mutual recognition agreement should be the flagship near-term deliverable of a practical EU-US cyber agenda. Its first tranche should focus on product assurance and conformity assessment: mutual reliance on competent conformity assessment bodies, acceptance of test results for agreed cybersecurity requirements in clearly defined product categories, and technical mapping of requirements, test methods, documentation and oversight practices. Future tranches could follow where equivalence can be demonstrated and where there is a clear industry need.

The first proof of concept should build on the existing conformity assessment route under the 1998 EU-US Mutual Recognition Agreement and the EU Radio Equipment Directive ("RED"). This would allow the EU and the US to test a limited, product-focused approach with legal, standards and conformity assessment expertise built in from the outset.

Restarting the EU-US Cyber Dialogue should support this agenda. The Dialogue should have a results-oriented mandate, structured industry input and dedicated tracks on response and recovery, emerging technologies and practical burden reduction.

DIGITALEUROPE calls on EU and US policymakers to:

- **launch a phased EU-US cybersecurity mutual recognition agreement work programme,** with a first deliverable focused on product assurance and conformity assessment;
- **leverage input from industry and experts into the design and implementation process;**
- **leverage international standards** as the starting point for technical alignment on key areas like incident reporting and mandate a joint requirements-mapping exercise where gaps remain;
- **prioritise mutual reliance on competent conformity assessment bodies and acceptance of test results** for agreed cybersecurity requirements in clearly defined product categories;
- **explore a proof of concept** linked to the existing **EU-US mutual recognition agreement framework and RED-covered cybersecurity requirements**;
- **restart the EU-US Cyber Dialogue** with clear deliverables, accountability and institutional firebreaks, including a **dedicated cyber response coordination track**, so that progress on cybersecurity mutual recognition can proceed in parallel with wider digital policy discussions.

DIGITALEUROPE
Rue de la Science, 37, B-1040 Brussels
+32 2 609 53 10 ▶ Info@digitaleurope.org
▶ www.digitaleurope.org
EU Transparency Register: 64270747023-20

@DIGITALEUROPE DIGITALEUROPE digitaleurope_org

Table of contents

Why EU-US cyber cooperation needs a practical way forward

EU-US cyber cooperation must move from broad political alignment to practical delivery. The EU and the US have the world's largest bilateral trade and investment relationship, with EU-US trade in goods and services reaching €1.6 trillion in 2024 and more than €4.2 billion crossing the Atlantic every day[1]. When cybersecurity rules fragment across a relationship of that scale, companies face higher costs, slower product launches and less time for the security work that most directly protects users and infrastructure.

Both sides are trying to raise security baselines, strengthen resilience and protect users. The problem is that similar policy goals are often pursued through separate processes, documentation expectations, testing pathways, conformity assessment procedures and reporting workflows. For companies operating across both markets, cybersecurity compliance can become a parallel workstream alongside cybersecurity itself. That is why mutual reliance on competent conformity assessment bodies and acceptance of test results is critical, for example in the context of NIS2 Directive compliance efforts.

The window for action is time-sensitive: without a concrete track, the cyber mutual recognition agreement risks being absorbed into broader EU-US discussions on trade and digital policy, rather than delivered as a practical outcome.

This fragmentation sits on top of an already expensive threat environment. According to industry estimates, the global average cost of a data breach reached approximately $4.44 million in 2025[2]. ENISA's 2025 NIS Investments report found that median cybersecurity spending in Europe was €1.5 million, cybersecurity represented 9 per cent of IT budgets, while 76 per cent reported difficulties attracting cybersecurity professionals.[3] Every unnecessary duplicate test, repeated technical file or parallel reporting process competes with investment in product security, vulnerability management, threat detection, incident response and recovery.

Product assurance is a clear example. A manufacturer selling connected products in both markets may need to prepare separate documentation, engage with different conformity assessment bodies and repeat similar testing even where the underlying cybersecurity outcome is comparable. The EU and the US already recognised this problem through the Joint CyberSafe Products Action Plan, which aims to advance technical cooperation towards mutual recognition of cybersecurity requirements for consumer IoT products.[4] This work should now be picked up and extended as part of a targeted cyber mutual recognition agreement.

Future tranches could explore the technical mapping of selected EU and US cybersecurity certification schemes, including cloud security where relevant. The objective would not be full identity between schemes, but to enable mutual recognition where equivalence can be demonstrated and to limit additional checks to clearly identified gaps.

Incident reporting creates a related but different burden. When a serious cyber incident occurs, companies need to focus on containment, business continuity, customer protection and recovery. Divergent reporting timelines, thresholds, templates and authorities can force legal, compliance and security teams to run several parallel processes during the most sensitive phase of an incident. While the priority is to

[1] https://commission.europa.eu/topics/trade/eu-us-trade-deal_en.
[2] https://www.ibm.com/reports/data-breach.
[3] https://www.enisa.europa.eu/news/whats-driving-cybersecurity-investments-and-where-lie-the-challenges.
[4] https://digital-strategy.ec.europa.eu/en/news/eu-and-united-states-enhance-cooperation-cybersecurity.

harmonise reporting obligations within the EU, future alignment with similar US structures should be a consideration.

A first deliverable: cyber mutual recognition

The August 2025 EU-US joint statement[5] gives the mutual recognition agreement track a stronger basis than previous cyber cooperation efforts. It commits the EU and the US to negotiate a cybersecurity mutual recognition agreement and reaffirms that US conformity assessment bodies can be designated as EU notified bodies under the telecommunications sectoral annex of the 1998 EU-US mutual recognition agreement for all RED essential requirements, including cybersecurity.[6]

Mutual recognition is an established trade tool. The EU describes mutual recognition agreements as instruments that facilitate market access by allowing one party to accept conformity assessment results, such as testing or certification, performed by designated conformity assessment bodies in the other party.[7] The National Institute of Standards and Technology ("NIST") similarly describes telecommunications mutual recognition agreement as government-to-government agreements that allow parties to recognise competent conformity assessment bodies and accept their results for regulatory purposes.[8]

A cyber mutual recognition agreement should apply that logic to cybersecurity product assurance where outcomes are equivalent. Its purpose should be to identify where companies can rely on recognised technical evidence instead of repeating equivalent assessment work. **The objective is not to replicate one side's regulatory model on the other**, but to identify where trusted technical evidence can be reused to deliver equivalent cybersecurity assurance with less duplicative compliance.

A credible first tranche should define the product categories that are in scope; map the relevant cybersecurity requirements, test methods, documentation expectations and vulnerability-handling obligations; identify which technical artefacts can be reused, such as test reports, technical files, certification evidence or declarations of conformity; and set the conditions for relying on conformity assessment bodies, including accreditation, designation, oversight and withdrawal where performance is not adequate.

Mutual recognition will only be credible if authorities can rely on the competence of assessment bodies, the quality of test results, the clarity of technical documentation and the effectiveness of oversight. **Industry, standards experts, conformity assessment bodies, accreditation bodies and test laboratories should therefore be involved from the outset.**

The EU Cyber Resilience Act (CRA) and the US Cyber Trust Mark illustrate why technical mapping is needed. The CRA creates a horizontal EU framework for products with digital elements, with different conformity assessment routes depending on the product category.[9] The Cyber Trust Mark is a voluntary labelling programme for wireless consumer internet of things products.[10] These systems are not identical, but that is precisely why the first phase should test equivalence at the level of requirements, evidence and assurance outcomes. A similar mapping exercise could later assess the relationship between the US

[5] Joint Statement on a United States-European Union framework on an agreement on reciprocal, fair and balanced trade - Trade and Economic Security
[6] Agreement on Mutual Recognition between the European Community and the United States of America
[7] https://single-market-economy.ec.europa.eu/single-market/goods/international-aspects-single-market/mutual-recognition-agreements_en.
[8] https://www.nist.gov/mutual-recognition-agreements-mras.
[9] https://digital-strategy.ec.europa.eu/en/policies/cra-conformity-assessment.
[10] https://www.govinfo.gov/content/pkg/FR-2024-07-30/pdf/2024-14148.pdf.

Secure Software Development Framework and relevant secure development lifecycle obligations under the Cyber Resilience Act.

The most practical proof of concept should build on the 1998 EU-US mutual recognition agreement and RED. The 1998 agreement already includes a telecommunications sectoral annex, and NIST explains that qualified US conformity assessment bodies may apply through its Telecom MRA Programme Office to become notified bodies under RED.[11] The August 2025 joint statement explicitly links that route to the cyber mutual recognition agreement discussion.

RED provides a useful starting point because cybersecurity requirements are already being applied to certain categories of radio equipment. Delegated Regulation (EU) 2022/30 applies RED essential requirements on network protection, protection of personal data and privacy, and protection from fraud applicable to specific categories of radio equipment. These requirements apply from 1 August 2025 until 11 December 2027, when CRA replaces RED cybersecurity requirements.[12] The Commission has also adopted harmonised standards supporting these RED cybersecurity requirements, which are reused in the CRA standards context.[13]

This does not mean that the 1998 mutual recognition agreement can automatically become the full legal vehicle for a cyber mutual recognition agreement. It was designed around conformity assessment in defined product sectors, not the full cybersecurity policy landscape. That limitation is also its value. A first cyber-related tranche should be framed precisely as a conformity assessment and product assurance exercise, providing a strong basis for future measures addressing cybersecurity requirements or certification schemes for which equivalence can be demonstrated.

The EU and the US should therefore use the telecom/RED route as a test case. The immediate task should be to assess which RED-covered requirements and product categories could support mutual reliance in practice. If the model works, it could provide a basis for considering additional product categories. If it does not, the exercise would still create a useful technical map of where requirements diverge and what would need to change.

The negotiation should be launched politically through the relevant EU-US cyber and trade channels, but implementation should stay grounded in conformity assessment practice. The Joint Committee and sectoral annex processes under the 1998 mutual recognition agreement should be explored as possible institutional vehicles, without prejudging whether the final architecture requires a new annex, an amendment, an implementing decision or another negotiated instrument. [14] [15] The key is to start from a tested route and a product assurance outcome.

[11] https://www.nist.gov/standardsgov/us-eu-mra-and-us-eea-efta-states-mutual-recognition-agreements
[12] Commission Delegated Regulation (EU) 2022/30, which applies RED essential requirements in Art. 3(3), points (d), (e) and (f), to certain categories of radio equipment.
[13] https://op.europa.eu/en/publication-detail/-/publication/16a8f500-deab-11ef-be2a-01aa75ed71a1/language-en
[14] https://eur-lex.europa.eu/EN/legal-content/summary/eu-united-states-of-america-mutual-recognition-agreement-mra.html.
[15] https://eur-lex.europa.eu/eli/dec/2019/559/oj/eng

A broader but disciplined transatlantic cyber agenda

Restarting the EU-US Cyber Dialogue should support the mutual recognition agreement and the broader agenda by focusing on concrete outputs. It should not become a general forum for restating shared cyber priorities. **It should operate through a clear work programme with defined deliverables, responsible agencies, timelines, industry input, and reporting.**

Incident response and recovery should be a dedicated track within that work programme, focused on operational interoperability: faster and more predictable coordination before, during and after serious cross-border incidents. **It should bring together the relevant EU and US operational actors.** On the EU side, this should involve the Computer Security Incident Response Teams (CSIRTs) Network, ENISA, the European Cyber Crises Liaison Organisation Network (EU-CyCLONe) and the Commission, building on the EU Cyber Blueprint. On the US side, the operational counterpart should be CISA/DHS, with NIST involved on standards, frameworks and technical alignment.

This track should develop practical outputs: identified contact points, common information categories, channels for sharing technical indicators and forensic artefacts, and principles for public communication when incidents affect users, supply chains or critical services on both sides of the Atlantic. At EU level, a single reporting entry point and further harmonisation of underlying obligations and timelines should come first. This work should be designed with future EU-US interoperability in mind, so that simplified European reporting structures do not need to be revisited soon after they are completed.

The private sector must be central. Companies are often the first to detect, analyse and contain incidents affecting their networks, products or services. CISA's Joint Cyber Defense Collaborative shows the value of public private cooperation for incident management, threat information exchange and coordinated guidance.[16] The 2023 ENISA-CISA Working Arrangement also provides a basis for deeper transatlantic cooperation on capacity-building, best practice exchange and situational awareness.[17]

The broader agenda should also look ahead. Cybersecurity requirements will increasingly shape artificial intelligence, quantum technologies, connected products and the digital infrastructure that supports them.

Frontier cyber-capable AI models make early coordination more urgent: controlled-access initiatives for defensive cyber use show that advanced models can accelerate vulnerability discovery, but they also raise practical questions about trusted access, coordinated disclosure, patch deployment and liability[18]. The EU and the US should use the Cyber Dialogue to compare lessons learned early and develop shared principles for defensive access governance, vulnerability management and safeguards for cyber-capable AI models.

Post-quantum cryptography is another practical area for coordination. NIST finalised its first three post-quantum cryptography standards in 2024,[19] and EU Member States, supported by the Commission, issued a coordinated roadmap for the transition to post-quantum cryptography in June 2025.[20] **Early EU-US coordination can reduce uncertainty and avoid fragmented assurance practices.**

[16] https://www.cisa.gov/ciscp.
[17] https://www.enisa.europa.eu/news/cisa-and-enisa-enhance-their-cooperation.
[18] https://www.anthropic.com/glasswing ; https://openai.com/index/scaling-trusted-access-for-cyber-defense ; https://www.war.gov/News/releases/release/Article/4475177/classified-networks-ai-agreements.
[19] https://www.nist.gov/node/1856616.
[20] https://digital-strategy.ec.europa.eu/en/library/coordinated-implementation-roadmap-transition-post-quantum-cryptography.

FOR MORE INFORMATION, PLEASE CONTACT:

Joël Guschker

Associate Director for International Affairs & Trade Policy

joel.guschker@digitaleurope.org

Hanna Harrison

Associate Director for Resilience & Critical Infrastructure

hanna.harrison@digitaleurope.org

Omar Dhaher

Technical Associate Director for Standardisation & Compliance Policy

omar.dhaher@digitaleurope.org

About DIGITALEUROPE

DIGITALEUROPE is the leading trade association representing digitally transforming industries in Europe. We stand for a regulatory and investment environment that enables European digitalising businesses across multiple sectors and citizens to prosper from digital technologies. We wish for Europe to grow, attract and sustain the world's best digital talents, investment and technology companies. Together with our members, we shape industry positions on all relevant policy matters, and contribute to their development and implementation. Our membership represents over 56,000 businesses who operate and invest in Europe. It includes corporations and scaleups who are global leaders in their field of activity, as well as national trade associations from across more than 30 European countries.