

An EU-U.S. Mutual Recognition Agreement on Cybersecurity

Why it matters and what it should address

The Issue: Fragmented Cybersecurity Regulations

There is growing international recognition that the global fragmentation of cybersecurity regulations is a strategic challenge, with the Information and Communication Technology (ICT) industry facing an increasing patchwork of regulatory approaches. According to a 2024 report from the Office of the U.S. National Cyber Director, Chief Information Security Officers (CISOs) now report spending 30-50% of their time on regulatory compliance activities across multiple regulatory regimes and jurisdictions, diverting resources away from combatting cyber threats¹.

In April 2025, a coalition of CISOs from over 50 global companies – including TTA members Microsoft, SAP and AWS – wrote to G7 and Organisation for Economic Co-operation and Development (OECD) member states to warn that this growing regulatory fragmentation is undermining companies' cyber defense operations, preventing the implementation of consistent security measures across different jurisdictions, and adding complexity to time-sensitive incident response activities².

This burden carries a mounting cost at precisely the wrong moment, diverting limited cybersecurity resources away from operational security and risk reduction toward compliance. Today AI-enabled cyber attacks are accelerating in both scale and sophistication, and the window of opportunity to harden defences before AI capabilities shift in attackers' favour is narrowing. Longstanding vulnerabilities – unpatched software, excessive permissions, weak authentication, and technical debt in legacy systems – are now exposed to adversaries with AI-augmented exploitation capabilities, while security teams, particularly those guarding critical infrastructure, remain historically under-resourced. Regulatory fragmentation compounds this by consuming the engineering, legal and security capacity that organisations need to redirect toward active defence—including raising the security bar for what they buy, build and deploy. The status quo is not sustainable as a security posture.

The challenge extends beyond individual organisations. AI-enabled threats do not respect jurisdictional boundaries. Critical infrastructure – hospitals, energy grids, water treatment facilities, financial systems – on which citizens depend is exposed to adversaries that operate globally and increasingly leverage AI to find and exploit vulnerabilities faster than defenders can respond. Addressing this requires a collective response: coordinated action across industry and governments that spans borders. Yet the current regulatory environment actively impedes this. When defenders in different jurisdictions must maintain separate and often competing compliance frameworks, navigate divergent certification pathways, and meet inconsistent incident reporting requirements, the result is a fragmented defence posture that benefits attackers and

¹ [See ONCD report here.](#)

² [See letter here.](#)

penalises defenders. Moreover, restrictions on cross-border data flows, particularly security telemetry and intelligence, further compound this problem by limiting the ability of defenders to share threat intelligence, coordinate incident response, and deploy consistent security measures across jurisdictions – effectively creating blind spots that adversaries can exploit.

In addition to undermining security outcomes, 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 borders³. 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 Trade⁴.

The OECD's *Towards international coherence of cybersecurity regulations* report (2026)⁵ 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, harmonizing incident reporting requirements and building a common cybersecurity taxonomy. In parallel, policymakers are beginning to incorporate regulatory simplification and interoperability objectives into cybersecurity policy and regulatory reform efforts.

This creates a unique policy environment and window of opportunity for advancing international alignment efforts on cybersecurity, including through mutual recognition agreements (MRAs). In the U.S., the 2026 National Cyber Strategy⁶ identified streamlining cybersecurity regulation as a domestic priority, while the European Union's (EU) Digital Omnibus⁷ and Cybersecurity Act⁸ simplification discussions similarly reflect growing interest in reducing overlapping requirements and improving interoperability. Australia's 2026-2028 Horizon 2 strategy⁹ emphasizes international regulatory alignment as part of its approach to strengthening digital resilience.

In March 2026, Singapore and Japan signed a Memorandum of Cooperation for the mutual recognition of their respective IoT cybersecurity labelling schemes – Singapore's Cybersecurity Labelling Scheme (CLS) and Japan's JC-STAR.¹⁰ Similarly in October 2024, Singapore signed Mutual Recognition Arrangements with South Korea and Germany to mutually recognize national cybersecurity labels for consumer IoT products.¹¹ Moreover, ASEAN member states have concluded negotiations on the ASEAN Digital Economy Framework Agreement – the world's first region-wide digital economy governance pact – which includes cybersecurity cooperation. Collectively, these developments underscore a rare convergence of political attention, policy reform cycles, and industry engagement that creates a meaningful opportunity to drive greater compatibility, reciprocity, and risk-based alignment before fragmentation becomes further entrenched.

³ [See WTO report here.](#)

⁴ Ibid.

⁵ [See OECD report here.](#)

⁶ [See U.S. National Cyber Strategy here.](#)

⁷ [See EU Digital Omnibus here.](#)

⁸ [See EU Cybersecurity Act here.](#)

⁹ [See Australia's 2026-2028 Horizon 2 strategy here.](#)

¹⁰ [See MRA between Singapore and Japan here.](#)

¹¹ [See MRA between Singapore, Germany, and the Republic of Korea here.](#)

Harnessing the momentum created by this policy focus on simplification of cybersecurity requirements is vitally important. Without stronger international efforts, regulatory fragmentation will continue hindering cross-border trade, slowing technology adoption, and diverting resources away from cyber defenders. Delivering an EU-U.S. cybersecurity MRA would be a critical first step to promote greater international harmonization, and the TTA supports extending such initiatives to other regions.

The Opportunity: the U.S.-EU Joint Statement and a cybersecurity MRA

The EU and the U.S. are the world's largest digital economies, and account for over \$5 trillion in digital trade annually¹². Both jurisdictions have developed extensive but divergent frameworks to address cybersecurity risks, and companies operating across both jurisdictions increasingly face duplicative certification and testing, parallel reporting requirements and audits, and redundant conformity assessments. These duplicative requirements divert time and effort away from the technical, operational and organizational security work that matters most.

The August 2025 U.S.-EU Joint Statement¹³ included a commitment to negotiating a cybersecurity MRA. This MRA represents an important opportunity to:

1. **Establish a baseline of mutual trust.** The MRA should recognize that companies headquartered in or operating from either jurisdiction should not face automatic disqualification or exclusion from market access on the basis of nationality or country of origin.
2. **Align cyber incident reporting requirements.** Advance greater consistency in cyber incident reporting, including shared definitions and timelines, reducing duplicative obligations while enabling faster, more coordinated cross-border incident response. Once more consistent, this could also help provide a basis and existing mechanism for reporting AI security incidents. Recent U.S. Government Accountability Office (GAO) findings¹⁴ highlight the scale of the challenge, identifying overlapping federal cybersecurity reporting requirements administered across multiple agencies.
3. **Promote technical criteria that ensure technology providers are assessed on demonstrated security capabilities.** Assessment criteria should be grounded in demonstrated security capacity and technical controls rather than blanket exclusions of nationality or headquarter location. Where operational-control, or data-residency requirements are determined necessary for specific high-risk categories, they should be defined transparently, applied only following a risk-based assessment, and subject to periodic review. Any such requirements should be subject to independent judicial oversight, to provide legal accountability and transparency.
4. **Reduce duplicative compliance burdens.** This would enable companies to reuse technical evidence to deliver equivalent cybersecurity assurance across both markets, freeing resources for frontline cybersecurity operations.

¹² [See WTO data here.](#)

¹³ [See U.S.-EU Joint Statement here.](#)

¹⁴ [See GAO report here.](#)

5. **Provide global leadership on regulatory harmonization.** At this moment, a demonstration that the world's two largest regulatory blocs can achieve interoperability would be exceptionally powerful. It would create a proof point for the kind of regulatory cooperation the OECD is working to systematize globally.
6. **Convert emerging policy consensus into lasting regulatory architecture.** Across industry, government, and multilateral bodies, there is a growing shared assessment of the AI-enabled threat landscape and the imperative for a collective response. An EU-U.S. MRA would translate that convergence into durable policy, demonstrating that the world's leading democratic economies can align on both the threat assessment and the regulatory response.

Policy Recommendations: What the MRA Should Include

While the U.S.-EU Joint Statement included a commitment to an MRA on cybersecurity, it left the question of scope and ambition for subsequent negotiations. The first step in this process should be to confirm the intention to go beyond a narrow, technical process that focuses solely on specific conformity assessments and notified bodies for a limited range of products.

While product-level mutual recognition can be useful, limiting the MRA's scope to this would miss the far greater opportunity, which is a comprehensive framework that drives broader convergence on trust-based cybersecurity requirements, especially in today's world when the AI threat environment is evolving faster than regulatory processes. As the European Commission advances the implementation of existing cybersecurity legislation and seeks greater alignment, coherence, and effectiveness across the EU cybersecurity framework through the revision of the Cybersecurity Act, and President Trump's March 2026 *Cyber Strategy for America* highlighting the need to "streamline cyber regulations to reduce compliance burdens, address liability, and better align regulators and industry globally"¹⁵, there is a clear opportunity for this.

This is a unique and urgent window of convergence in EU-U.S. policymaking. It creates an opening to shape vertical and horizontal cybersecurity requirements before they become crystallized under legal frameworks that do not keep pace with the cyber threat environment, technological innovation, or market developments.

The following principles-driven practical outcomes should form the aims of an EU-U.S. cybersecurity MRA as a central pillar within a broader regulatory cooperation structure:

1. **Adherence to internationally recognized cybersecurity and resilience standards.** Where there are binding regulations with similar scope in both the U.S. and EU, direct reciprocity should be sought, and, where available, internationally recognized standards (e.g. ISO standards) should be accepted by both parties as a basis for satisfying compliance requirements. However, effective recognition must also account for a structural difference between both systems: EU cybersecurity requirements are typically codified in binding, cross-sectoral statutes with designated competent authorities, while U.S. requirements are more often sector-specific, like the Federal Risk and Authorization Management Program (FedRAMP), or built on voluntary frameworks such as the NIST Cybersecurity Framework. The MRA should not assume symmetry that does not exist. Instead, it should specify precisely how adherence to a voluntary U.S. framework can satisfy a binding EU statutory

¹⁵ [See strategy here.](#)

obligation, and alternately, what assurance the EU side provides that is reasonable with the U.S.'s more decentralized regulatory structure..

2. **Supply chain security alignment.** The EU and the U.S. should align their approaches to supply chain security based on objective, risk-based criteria. In particular, an “assess once, reuse many times” model similar to the U.S.’s FedRAMP would be beneficial where ICT providers are audited once based on technical criteria, the results are stored in a secure repository and (regulated) customers can rely on that assessment.
3. **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 public procurement on both sides of the Atlantic. In particular, the U.S.’s FedRAMP and the EU’s draft Cybersecurity Certification Scheme for Cloud Services (EUCS)¹⁶ should recognize equivalence between their respective technical controls, and avoid duplicative evaluation processes for companies operating across both jurisdictions. Where possible, they should also allow for the re-use of evidence by qualified providers.
4. **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. EU-U.S. alignment on AI security standards also would prevent a new layer of transatlantic fragmentation from forming in a domain where the security stakes are high and growing.
5. **Procedural harmonization.** Incident reporting timelines, definitions, and a single early-warning notification format accepted across both jurisdictions, ideally aligning reporting thresholds, building on the EU-U.S. Cyber Dialogue, to enable coherent and timely cross-border response. Fragmented reporting requirements mean that cross-border incidents generate duplicative, asynchronous regulatory obligations that slow the response at precisely the moment when speed matters most, diverting operational attention from containment and remediation toward regulatory process management.
6. **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.
7. **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. Audits and certification evidence, such as vulnerability details, incident records, and audit trails, frequently involve personal data. Any framework for reuse of such evidence across jurisdictions must specify how it conforms with existing data transfer mechanisms to avoid

¹⁶ This recommendation recognizes that the EU’s draft Cybersecurity Certification Scheme for Cloud Services (EUCS) is still under discussion, specifically concerning assurance-level requirements for the most sensitive workloads. The MRA should be designed to accommodate whatever form EUCS ultimately takes, and is without prejudice to that internal EU process.

creating parallel, undefined channels for the movement of security-related personal data outside the safeguards already established for cross-border transfers.

8. **Mutual recommendation of AI Cyber Defence tool approvals.** The MRA should include dedicated provisions to remove regulatory and procurement barriers to the cross-border deployment of AI-powered cyber defence tools. It should make sure that AI-powered defence is accessible and deployable, especially for critical-infrastructure operators.

This paper starts from the basic assumption that closer cooperation and regulatory alignment is now an imperative, particularly if the EU and the U.S. are to develop a framework that unites both sides in pursuit of the world's most robust operational practice for cybersecurity. The recommendations above set out a route of pragmatic cooperation and compromise on mutual recognition that would preserve the important balance between aligned practice and the ultimate regulatory prerogatives and autonomy of both sides. It would develop a robust legal base for coordination, while respecting and protecting existing and ongoing data regulation and the unique features of both frameworks. It would signal close EU-U.S. strategic alignment at a time when such a signal has never been more important.

As such, the significance of this approach extends beyond cybersecurity. As governments develop new rules for AI, they face many of the same risks of regulatory fragmentation, including divergent requirements that can complicate cross-border operations and cooperation. An EU-U.S. cybersecurity MRA can therefore serve as an important proof point, demonstrating how mutual recognition, interoperability, and practical regulatory cooperation can help governments pursue shared policy objectives without requiring identical regulatory frameworks.