

SYMPOSIUM CONTRIBUTION

Allocating Liability for AI-Driven Cyber Harm: A Risk-Based Framework for Indiana, Informed by European Union (EU) and U.S. Models

Alvin D. Oliver II*

Abstract

Artificial intelligence now operates on both sides of the cybersecurity landscape, defending critical systems while also enabling novel forms of attack, yet the liability doctrines meant to allocate responsibility for the resulting harms were not designed for systems that continue to learn and change after deployment. This article argues that product liability, negligence, and contract law each fail to provide a stable basis for assigning responsibility when AI-driven cyber incidents occur, leaving developers, deployers, and the public exposed to a growing accountability gap. Comparing the regulatory approaches taken by the United States, the European Union, and China, the article evaluates each jurisdiction's institutional capacity for reciprocal commitments, its ability to export regulatory norms beyond its own borders, and the transparency required to sustain cross-border accountability. Drawing on this comparative analysis, the article proposes a targeted, risk-based liability framework for the state of Indiana, applicable to high-risk AI systems deployed in sectors such as health care, finance, and critical infrastructure. The proposed framework allocates responsibility between developers and deployers, imposes baseline cybersecurity and documentation obligations, creates safe harbours for organizations acting in good faith, and establishes incident-reporting requirements. In doing so, the article offers Indiana a workable model for AI accountability that does not require, and need not wait for, a comprehensive federal AI liability statute.

Keywords: AI liability, cybersecurity, comparative AI governance, high-risk AI systems, Indiana law

A Introduction

At 2:13 a.m., a hospital network loses access to its electronic health records after an AI-assisted ransomware attack bypasses automated intrusion defences. Within hours, surgeries are delayed, ambulances are rerouted and patient data appear for

* Alvin D. Oliver II, J.D., Indiana University Robert H. McKinney School of Law, 2026; M.S., Cybersecurity Risk Management, Indiana University Bloomington, 2026.

sale online. The hospital blames its cybersecurity vendor. The vendor blames flaws in the underlying AI model. The model developer points to improper deployment by the hospital's cloud provider. Meanwhile, regulators, insurers and patients are left asking the same question: who is legally responsible when artificial intelligence causes or enables cyber harm?

Artificial intelligence now operates on both sides of the cybersecurity battlefield. AI systems can detect intrusions, filter malicious activity or triage incidents, but they can also be used to probe systems, generate explicit code and optimize cyberattacks at a scale that far exceeds human capabilities. At the same time, organizations increasingly rely on AI-driven systems to perform intrusion detection, behavioural monitoring and incident response—functions traditionally requiring human oversight. As these systems become more autonomous and integrated into critical infrastructure, failures are no longer confined to isolated technical errors. Instead, AI-driven cyber incidents can produce cascading economic, operational and societal consequences across multiple jurisdictions within moments. Existing liability doctrines, however, were not designed for adaptive learning systems operating across complex international digital environments.

Current approaches to AI governance remain fragmented and incomplete. In the United States, policymakers have largely relied on voluntary frameworks, state privacy laws, critical infrastructure standards and agency guidance rather than a comprehensive federal AI liability law.¹ The National Institute of Standards and Technology (NIST) released the AI Risk Management Framework (AI RMF) to provide organizations with a voluntary framework for identifying, assessing, and managing AI-related risks throughout the AI lifecycle.² But because that framework is voluntary, it does not create an enforceable duty or a private right of action. As a result, AI-related cyber harm is left mostly to contract, tort or scattered regulatory obligations that were not designed for these incidents.

By contrast, the EU has moved towards a more detailed and sophisticated regulatory approach. The General Data Protection Regulation (GDPR), NIS2 Directive and AI Act together create a risk-based compliance structure that imposes concrete obligations on AI developers and deployers, especially for high-risk systems that affect fundamental rights or critical infrastructure.³ Article 45 of the GDPR and the EU's adequacy regime also show how European law structures cross-border digital relationships.⁴ Although the United States has obtained limited adequacy recognition for certain commercial transfers through the EU–U.S.

1 *Data Protection in the United States*, DLA Piper (6 February 2025), <https://www.dlapiperdataprotection.com/?c=US>.

2 *Artificial Intelligence Risk Management Framework (AI RMF 1.0)*, Nat'l Inst. of Standards & Tech., NIST AI 100-1 (January 2023), <https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.100-1.pdf>.

3 *AI Act*, European Commission, <https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai> (last visited 22 May 2026).

4 *FAQs—General*, Data Privacy Framework Program, <https://www.dataprivacyframework.gov/program-articles/FAQs-General> (last visited 22 May 2026); *Adequacy Decisions*, European Commission, https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en (last visited 22 May 2026).

Data Privacy Framework (DPF), the broader picture remains one of partial and conditional alignment rather than full convergence.⁵

China occupies an increasingly important, but more complex corner of this landscape. It has been one of the first jurisdictions to adopt binding measures specific to generative AI, emphasizing consent control, security review and alignment with core state-defined values.⁶ At the same time, opacity in adjudication, expansive state secrets rules and the central role of national security considerations make it difficult to evaluate how these measures translate into predictable liability or reciprocal obligations for foreign actors.⁷ That reality is useful context for Indiana, which increasingly relies on AI systems built and deployed by global technology firms operating across all three regulatory environments.

This article argues that Indiana should adopt a risk-based liability and cybersecurity framework for high-risk AI systems that combines the EU's clearer accountability standards with the flexibility of the current U.S. approach. Existing American frameworks rely too heavily on voluntary guidance and fragmented doctrines, while the EU model demonstrates how enforceable obligations for developers and deployers can create more predictable accountability. By borrowing selectively from both systems, Indiana can establish clearer cybersecurity duties for high-risk AI systems without unnecessarily stifling innovation.

Although this article focuses on Indiana, AI-driven cyber harm is not confined by state or national borders. Indiana hospitals, financial institutions, infrastructure operators and businesses increasingly rely on AI systems integrated into global digital networks and supply chains. As a result, failures originating outside Indiana can still produce substantial harms within the state. Indiana therefore has a strong interest in drawing on the most workable elements of emerging international governance frameworks while designing a liability structure tailored to state-level enforcement realities.

This article proceeds in four parts. Part B maps the liability gaps exposed by AI-driven cyber incidents; explains why traditional tort, product liability and contract doctrines struggle to handle these systems; and compares U.S., EU and Chinese regulatory approaches with attention to what Indiana should borrow and what it should reject. Part C evaluates the institutional capacity of those systems to support reliable coordination, examining transparency, enforcement and norm exportability as criteria for determining which models Indiana can credibly draw upon. Part D proposes a targeted, risk-based Indiana framework for

5 European Commission, *supra* note 4.

6 Tim Hickman et al., *AI Watch: Global Regulatory Tracker*, White & Case LLP, <https://www.whitecase.com/insight-our-thinking/ai-watch-global-regulatory-tracker> (last visited 22 May 2026).

7 Feifei (Andrea) Ren & John Davis, *China's Revised and More Stringent State Secrets Law Takes Effect*, Reuters (7 May 2024), <https://www.reuters.com/legal/legalindustry/chinas-revised-more-stringent-state-secrets-law-takes-effect-2024-05-07/>.

high-risk AI systems, addressing liability allocation, baseline cybersecurity obligations, safe harbours and incident reporting. Part E concludes.

B Liability Gaps in AI-Driven Cyber Incidents

AI-driven cyber incidents show the fundamental weakness in existing liability regimes. AI systems are frequently deployed across layered digital supply chains involving developers, integrators, cloud providers and end users.⁸ When harm occurs, existing doctrines often struggle to determine whether responsibility lies with design, deployment, post-deployment modification or some combination of the three.⁹ The result is not merely doctrinal uncertainty but a structural accountability gap in which existing law lacks a stable method for allocating loss when AI-driven cyber harms occur. These risks are especially significant in sectors such as health care, finance, transportation and critical infrastructure.

I How AI Creates Novel Cyber Harms

AI systems now meaningfully shape both offensive and defensive cyber operations.¹⁰ On the offensive side, machine learning models can automate vulnerability discovery, generate phishing content at scale and optimize attack timing and targeting in ways that exceed human capacity.¹¹ On the defensive side, AI increasingly performs intrusion detection–behavioural monitoring–incident response triage.¹² These same systems, however, can fail silently, misclassify threats or be manipulated through techniques such as prompt injection, data poisoning or model inversion.¹³

What distinguishes these failures from conventional software defects is not only scale but also agency ambiguity. An AI model may behave in ways that were neither explicitly programmed nor directly intended but were statistically foreseeable given the model's design, training data and implementation.¹⁴ This ambiguity complicates traditional inquiries into fault, intent and causation. In traditional software disputes, the relevant question is often whether a human actor introduced a defective line of code or failed to patch a known vulnerability. In the AI context, however, the more difficult question is whether a harmful outcome

8 Amrita Vasudevan, *Addressing the Liability Gap in AI Accidents*, Ctr. Int'l Governance Innovation (July 2023), https://www.cigionline.org/static/documents/PB_no.177.pdf.

9 *Id.*

10 Mark Pomerleau, *CYBERCOM Requests 2,660 Percent Increase in AI for Cyber Operations*, Breaking Defense, (12 May 2026), <https://breakingdefense.com/2026/05/cybercom-requests-2660-percent-increase-in-ai-for-cyber-operations/>.

11 *An Overview of Catastrophic AI Risk*, Ctr. for AI Safety, <https://safe.ai/ai-risk> (last visited 22 May 2026).

12 Kwaku Gyamfi Boamah et al., *Artificial Intelligence Integration in Cyber Incident Response Teams to Enable Faster Containment, Forensic Accuracy, and Resilient Business Continuity*, 17 Int'l J. Sci. and Rsch. Archive 1263, 1263 (2025).

13 Fayyaz Makhani, *The Hidden Risks of Relying on AI in Cybersecurity*, Viking Cloud (27 October 2025), <https://www.vikingcloud.com/blog/disadvantages-of-ai-in-cybersecurity>.

14 Andy Smith, *AI Model Misbehavior in 2026: Scheming, Reward Hacking, and What Comes Next*, Hatch-WorksAI (27 March 2026), <https://hatchworks.com/blog/gen-ai/ai-model-misbehavior/>.

reflects negligent design, inadequate deployment, foreseeable model behaviour or a system that evolved beyond the control of its original creator.

This problem is particularly acute in cybersecurity because the same AI system may function as both a defensive tool and a source of liability. A model trained to identify suspicious activity may also be repurposed, manipulated or degraded in ways that expose the very infrastructure it was designed to protect. Existing legal frameworks can generally identify a victim and a loss, but they struggle to furnish a stable basis for assigning responsibility when AI systems operate through layered and partially autonomous digital environments.

Recent disputes involving autonomous AI agents further illustrate these concerns. In 2025 and 2026, Amazon accused Perplexity AI's 'Comet' browser of using AI agents to access Amazon's platform and make purchases on behalf of users without authorization, resulting in litigation involving alleged computer fraud, unauthorized access and cybersecurity risks associated with autonomous AI behaviour.¹⁵ Amazon specifically argued that the AI agents created security risks because they were capable of operating within protected customer systems and accounts, while Perplexity characterized the dispute as an attempt to restrict emerging AI-agent technologies.¹⁶ The dispute illustrates how AI systems increasingly blur traditional distinctions between user conduct, platform access, developer responsibility and autonomous system behaviour.

II Breakdown of Traditional Liability Doctrines

1 Product Liability

Traditional product liability doctrine is an imperfect fit to serve AI systems that continue to evolve after deployment through updates, retraining or autonomous learning.¹⁷ Strict liability traditionally attaches to defective products placed into the stream of commerce, but AI models are frequently updated, retrained or fine-tuned after release.¹⁸ The relevant failure may therefore arise not at the moment of sale but after implementation, when the system has changed in ways that were not fully captured by the original design or testing process. Courts have also historically been reluctant to treat software, particularly non-embedded software, as a 'product' for strict liability purposes.¹⁹

15 Annie Palmer, *Amazon Wins Court Order to Block Perplexity's AI Shopping Agent*, CNBC (10 March 2026), <https://www.cnn.com/2026/03/10/amazon-wins-court-order-to-block-perplexitys-ai-shopping-agent.html>.

16 *Id.*

17 Mark A. Buiten, *Product Liability for Defective AI*, European Journal of Law and Economics (2024), <https://doi.org/10.1007/s10657-024-09794-z>.

18 Frances M. Green & Bryan Hahm, *Built to Blame: The Product-Service Divide and Emerging Liability for AI-Inflicted Harm*, N.Y. L.J. (21 April 2026), <https://www.ebglaw.com/insights/publications/built-to-blame-the-product-service-divide-and-emerging-liability-for-ai-inflicted-harm/>.

19 Erin M. Bosman et al., *Software Gains New Status as a Product Under Strict Liability Law*, Morrison & Forester (18 June 2025), <https://www.mofo.com/resources/insights/250618-software-gains-new-status-as-a-product-under-strict-liability-law> ("Traditionally, courts have been hesitant to treat software and other nontangible consumer goods as a 'product' for purposes of strict liability claims.

These limitations become even more significant when harm results from emergent behaviour inherent in complex AI systems rather than from a discrete defect. Unlike traditional product defects, AI-related harms may emerge from the interaction of training data, deployment conditions and post-deployment learning, making it difficult to determine both when the system became defective and which actor should bear responsibility. Product liability doctrine therefore struggles to map cleanly onto AI systems that continue evolving after deployment.

2 *Negligence and Software Liability*

Negligence-based frameworks face parallel challenges. Establishing breach requires identifying a standard of reasonable care, yet no widely accepted benchmark exists for AI cybersecurity practices, particularly in the United States.²⁰ In the absence of mandatory standards, developers and deployers can argue that compliance with voluntary frameworks reflects reasonable care, even when those frameworks are incomplete, aspirational or inconsistently applied.²¹ The absence of binding standards therefore becomes part of the reason liability is difficult to establish.

This problem is especially relevant in the AI context because reasonable care may depend on highly technical judgments regarding adversarial testing, monitoring, training data integrity and post-deployment governance.²² Courts are not institutionally well positioned to develop those standards retroactively after harm has already occurred. As a result, negligence claims may fail not because no one acted carelessly, but because the law lacks a stable reference point for evaluating whether the relevant conduct was reasonable at all. Without clearer regulatory baselines, liability remains fragmented, unpredictable and heavily dependent on after-the-fact litigation.

3 *Contractual Allocation and Its Limits*

In practice, liability for AI-related cyber harm is often allocated by contract.²³ Cloud service agreements, software licences and enterprise AI terms routinely disclaim consequential damages and shift responsibility downstream.²⁴ These arrangements

However, a recent decision from the U.S. District Court for the Middle District of Florida demonstrates courts' progressing willingness to consider AI software and applications as products under strict products liability principles.”).

20 Aidan Kierans et al., *Catastrophic Liability: Managing Systemic Risks in Frontier AI Development*, arXiv (1 June 2025), <https://arxiv.org/html/2505.00616v2>.

21 Matthew F. Ferraro et al., *NIST Releases Draft Framework for AI Cybersecurity, Solicits Public Comment: What Organizations Using or Deploying AI Should Know*, Crowell & Moring LLP (13 January 2026), <https://www.crowell.com/en/insights/client-alerts/nist-releases-draft-framework-for-ai-cybersecurity-solicits-public-comment-what-organizations-using-or-deploying-ai-should-know>.

22 Rafal Fryc, *Incentives or Obligations? The U.S. Regulatory Approach to Voluntary AI Governance Standards*, Future of Privacy Forum (18 March 2026), <https://fpf.org/blog/incentives-or-obligations-the-u-s-regulatory-approach-to-voluntary-ai-governance-standards/>.

23 Jennifer L. Brown, *The Expanding Prevalence of AI Clauses in Contracts*, Taft (18 November 2025), <https://www.taftlaw.com/news-events/law-bulletins/the-expanding-prevalence-of-ai-clauses-in-contracts/>.

24 *See id.*

may effectively allocate commercial risk between sophisticated parties capable of negotiating before any harm occurs, but they have significant limitations.

Most importantly, contract cannot fully address harms suffered by third parties, critical infrastructure operators or the general public.²⁵ A cyber incident affecting hospitals, patients, consumers or downstream network users may never be governed by the relevant software agreement at all. Contractual allocation also tends to disperse responsibility across multiple agreements within a complex digital supply chain, making accountability more difficult to trace when harm occurs. Contract may distribute commercial risk within that supply chain, but it does not create a coherent public framework for assigning responsibility when AI-driven cyber harms affect non-parties.

III Comparing Regulatory Approaches to Liability Gaps

1 United States

The United States has largely avoided imposing affirmative liability obligations on AI developers.²⁶ Federal policy emphasizes innovation and voluntary risk management, reflected in the NIST AI Risk Management Framework and sector-specific cybersecurity guidance.²⁷ Although these instruments encourage best practices, they do not create enforceable duties or clearly define what constitutes legally adequate AI governance.²⁸ As a result, liability determinations remain fragmented across tort, contract and regulatory frameworks.²⁹

That fragmentation has significant consequences. The American approach prioritizes innovation and market flexibility, but it does so at the cost of predictable accountability. By relying heavily on voluntary guidance and after-the-fact litigation, the current system leaves courts, businesses and injured parties without a stable framework for allocating responsibility when AI systems fail.³⁰ This lack of

25 *AI Terms and Indemnity in Commercial Contracts*, Margolis PLLC (31 December 2025), <https://www.margolispllc.com/post/ai-terms-and-indemnity-in-commercial-contracts>.

26 Avishay Klein & Nadine Liv, *US Senate Rejects AI Enforcement Moratorium: Legal Liability Applies to AI Companies*, Barnea (13 July 2025), https://barlaw.co.il/practice_areas/high-tech/ai-regulation/client_updates/us-senate-rejects-ai-enforcement-moratorium-legal-liability-applies-to-ai-companies/.

27 *AI Risk Management Framework*, Nat'l Inst. of Standards & Tech., <https://www.nist.gov/itl/ai-risk-management-framework> (last visited 22 May 2026).

28 Fryc, *supra* note 22.

29 *AI Enforcement Accelerates as Federal Policy Stalls and States Step In*, Morgan Lewis (2 April 2026), <https://www.morganlewis.com/pubs/2026/04/ai-enforcement-accelerates-as-federal-policy-stalls-and-states-step-in>.

30 *We're Not Ready for AI Liability*, AI Frontiers (16 February 2026), <https://ai-frontiers.org/articles/options-for-ai-liability>.

clarity is especially problematic in high-risk sectors where AI-driven failures may produce immediate operational, financial and public safety consequences.

2 European Union

The EU has moved closer to addressing AI-related liability indirectly through regulation.³¹ The AI Act's risk-based framework imposes mandatory obligations, such as risk management, data governance and post-market monitoring obligations, on providers and deployers of high-risk AI systems.³² When paired with GDPR, NIS2 and proposed AI liability reforms, the EU approach reduces uncertainty by linking technical governance to legal accountability.³³ That structure provides clearer prospective guidance than the current U.S. approach, although critics argue that the EU model risks imposing substantial compliance burdens and regulatory rigidity in a rapidly evolving technological environment.³⁴

The significance of the EU model is not that it fully resolves every liability question, but that it establishes clearer expectations before harm occurs. By imposing process-based obligations on high-risk systems, the EU framework makes later allocation of fault more predictable and coherent. Compliance does not eliminate liability, but it creates more meaningful baselines for evaluating whether developers and deployers acted reasonably.

3 China

China's regulatory approach emphasizes state oversight, content control and security review rather than private law liability.³⁵ While China has adopted binding measures for generative AI, enforcement discretion, opaque adjudication and the central role of national security complicate efforts to derive predictable liability standards.³⁶ Those characteristics make China a difficult model for reciprocal liability coordination, even though its growing role in AI development makes eventual engagement unavoidable.

31 *EU Updates Its Product Liability Regime: Important Considerations for Providers of AI Systems and Software*, Goodwin Procter LLP (February 2025), [https://www.goodwinlaw.com/en/insights/publications/2025/02/alerts-practices-aiml-eu-updates-its-product-liability-regime;AI as Product vs. AI as Service: Unpacking the Liability Divide in EU Safety Legislation](https://www.goodwinlaw.com/en/insights/publications/2025/02/alerts-practices-aiml-eu-updates-its-product-liability-regime;AI%20as%20Product%20vs.%20AI%20as%20Service:Unpacking%20the%20Liability%20Divide%20in%20EU%20Safety%20Legislation), IAPP (19 November 2025), <https://iapp.org/news/a/ai-as-product-vs-ai-as-service-unpacking-the-liability-divide-in-eu-safety-legislation>.

32 *AI Act*, *supra* note 3.

33 *Id.*

34 Oliver Roberts, *EU AI Act's Burdensome Regulations Could Impair AI Innovation*, BL (21 February 2025), <https://news.bloomberglaw.com/us-law-week/eu-ai-acts-burdensome-regulations-could-impair-ai-innovation>; *EU Parliament Publishes Report on Interaction Between EU Digital Regulations*, Morgan Lewis (19 November 2025), <https://www.morganlewis.com/blogs/sourcingatmorganlewis/2025/11/eu-parliament-publishes-report-on-interaction-between-eu-digital-regulations>.

35 *China Amends Cybersecurity Law and Incident Reporting Regime to Address AI and Infrastructure Risks*, Global Policy Watch (31 October 2025), <https://www.globalpolicywatch.com/2025/10/china-amends-cybersecurity-law-and-incident-reporting-regime-to-address-ai-and-infrastructure-risks>; Tim Hickman et al., *AI Watch: Global Regulatory Tracker – China*, White & Case LLP, <https://www.whitecase.com/insight-our-thinking/ai-watch-global-regulatory-tracker-china> (last visited 22 May 2026).

36 Ren, *supra* note 7.

China therefore serves more as a cautionary example than as a practical model for Indiana. It demonstrates that the existence of binding AI rules alone is insufficient. Effective accountability also requires transparency, predictable enforcement and meaningful procedural safeguards. Without those characteristics, cross-border cooperation and stable liability allocation become difficult to sustain.

IV *The Resulting International Accountability Gap*

The absence of harmonized liability standards creates a perverse incentive structure. Developers may design to the lowest enforceable standard, deployers may rely on contractual disclaimers and governments may exploit attribution uncertainty to avoid responsibility for AI-enabled cyber operations.³⁷ Without clearer allocation of responsibility, AI-driven cyber harms risk becoming normalized as regulatory externalities rather than legally cognizable injuries.

This problem is not merely one of incomplete regulation but also of structural accountability failure. AI systems are increasingly deployed in environments where errors can produce immediate and cross-border consequences, yet existing legal doctrines remain fragmented across jurisdictions and frameworks that were not designed for adaptive systems operating at scale.³⁸ While no jurisdiction has fully solved this problem, the comparative approaches adopted by the United States, EU and China reveal important lessons about accountability, flexibility and enforcement. As Parts C and D argue, Indiana can draw selectively from those systems to develop a more coherent liability and cybersecurity framework for high-risk AI governance.

C Institutional Capacity and Feasibility of AI Coordination

The liability gaps identified in Part B do not arise in a vacuum. They reflect deeper questions about which legal systems are capable of sustaining reciprocal, enforceable commitments on AI liability and cybersecurity. Some jurisdictions have adopted detailed governance frameworks but lack transparent enforcement, while others rely heavily on voluntary standards or post hoc litigation.³⁹ Before Indiana can sensibly borrow from foreign or federal models, it must evaluate not only what those systems require on paper but also whether their rules are transparent, enforceable and adaptable enough to function within Indiana's legal and regulatory environment.

37 *AI Vendor Liability Squeeze: Courts Expand Accountability While Contracts Shift Risk*, Jones Walker LLP (15 September 2025), <https://www.joneswalker.com/en/insights/blogs/ai-law-blog/ai-vendor-liability-squeeze-courts-expand-accountability-while-contracts-shift-r.html>; *Liability Rules and Standards*, Nat'l Telecomms. & Info. Admin., <https://www.ntia.gov/issues/artificial-intelligence/ai-accountability-policy-report/using-accountability-inputs/liability-rules-and-standards> (last visited 22 May 2026).

38 Mohamed Chawki, *Legal Foundations and Future Directions of AI-Enabled Cybersecurity: A Cross-Jurisdictional Analysis*, 12 Cogent Soc. Sci. 1, 1 (January 2026), <https://www.tandfonline.com/doi/full/10.1080/23311886.2026.2614015>.

39 *Global Fragmentation of AI Governance and Regulation*, Bloomsbury Intelligence & Security Inst. (13 February 2026), <https://bisi.org.uk/reports/global-fragmentation-of-ai-governance>.

I. Capacity for Reciprocal Commitments

Effective coordination on AI liability requires more than domestic regulation. It depends on whether legal systems can: (1) articulate clear compliance obligations; (2) enforce those obligations predictably; and (3) extend them credibly to foreign actors.⁴⁰ Systems that satisfy these conditions are better positioned to support reciprocal arrangements through formal agreements, mutual recognition mechanisms or de facto convergence around shared standards.⁴¹

The United States and the EU, despite meaningful differences in regulatory style, both satisfy these conditions. Both rely on transparent rulemaking processes, judicial review and relatively stable enforcement institutions. While the United States traditionally favours flexibility and sector-specific guidance, and the EU relies more on prescriptive mandates, both systems ground compliance in rule-of-law mechanisms that make regulatory obligations more predictable to outside actors. The institutional stability matters for Indiana because it makes federal and European standards more reliable reference points when designing state-level liability rules.

China presents a different institutional profile. Although China has adopted binding AI regulations and security-review mechanisms, enforcement discretion, limited judicial transparency and the central role of national security considerations make it difficult for foreign actors to assess how those rules will be applied in practice.⁴² The result is a system where formal obligations may not reliably signal actual enforcement risk. That gap between law on the books and law in action weakens China's suitability as a primary template for reciprocal liability or as a direct model for Indiana's framework.

II. Exportability of Regulatory Norms

A second dimension concerns norm exportability or whether a regulatory system can influence behaviour beyond its territorial borders. The EU has repeatedly demonstrated this capacity through market-access conditions, adequacy determinations and expansive digital governance requirements.⁴³ EU digital regulations frequently function extraterritorially without requiring formal treaties or explicit adoption by foreign legislatures.⁴⁴ Firms seeking access to EU markets often structure products, governance systems and compliance practices around European requirements even when operating elsewhere. This regulatory gravity gives the EU disproportionate influence in shaping global technology and cybersecurity baselines.

The United States exports regulatory influence less through prescriptive legislation than through the global dominance of its cloud providers, AI developers

40 *Ensuring a National Policy Framework for Artificial Intelligence*, White House (11 December 2025), <https://www.whitehouse.gov/presidential-actions/2025/12/eliminating-state-law-obstruction-of-national-artificial-intelligence-policy/>.

41 *See Generally Six AI Governance Priorities for 2026*, Partnership on AI (19 February 2026), <https://partnershiponai.org/resource/six-ai-governance-priorities/>.

42 Wu Yangyu, *China's AI Firms Hit Fragmented Global Rules as Overseas Expansion Gathers Pace*, Jiemian (28 December 2025), <https://m.jiemian.com/article/13821562.html>.

43 *See* Council Regulation (EU) 2016/679 (GDPR); Regulation (EU) 2024/1689 (AI Act).

44 *See id.*

and digital infrastructure companies.⁴⁵ U.S.-based AI models, cybersecurity vendors and cloud service providers are deeply embedded in global digital systems, allowing American technical practices and governance expectations to shape industry behaviour beyond U.S. borders. For Indiana, this means that both EU and U.S. approaches already exert de facto influence over many of the companies and technologies operating within the state.

China's regulatory norms, by contrast, remain more geographically bounded. Although Chinese firms play a growing role in global AI markets, China's AI governance model has not demonstrated the same ability to function as a widely adopted default in liberal democratic systems.⁴⁶ Political, legal and institutional differences limit the willingness of U.S. and European institutions to import Chinese standards wholesale. As a result, Chinese AI regulation is more relevant as a strategic constraint and source of competitive pressure than as a direct source of transplantable liability principles for Indiana.

III. Trust, Verification and Transparency

Trust and verifiability are also central to any sustainable AI liability framework. AI systems are difficult to audit in a fully transparent manner because disclosure of model weights, training data or security configurations may expose trade secrets or create additional cybersecurity vulnerabilities.⁴⁷ Coordination therefore depends heavily on procedural trust: confidence that participating jurisdictions will apply their rules in a reasonably transparent, predictable and reviewable manner even when aspects of the underlying technology remain opaque.⁴⁸

The United States and the EU possess institutional features that support this kind of procedural trust. Both systems provide mechanisms for independent audits, judicial review, regulatory appeals and external oversight.⁴⁹ Regulated entities can challenge agency action, while outside observers can often reconstruct the reasoning behind major regulatory decisions. Those mechanisms reduce uncertainty for outside actors and make it more plausible to rely on certifications, reporting obligations and safe-harbour structures that incorporate AI governance standards.

China's system provides a useful counterpoint. Centralized administrative control, expansive secrecy doctrines and the prominent role of national security limit the ability of external actors to verify enforcement practices or anticipate how AI-related rules will be interpreted in specific cases.⁵⁰ That opacity is not merely a

45 Center for AI Standards and Innovation (CAISI), Nat'l Inst. of Standards and Tech., <https://www.nist.gov/caisi> (last visited 22 May 2026).

46 Yangyu, *supra* note 42.

47 *Trade Secrets in the AI Era: Navigating Transparency Under the EU AI Act*, Herbert Smith Freehills Kramer (30 October 2025), <https://www.hsfkramer.com/insights/2025-10/trade-secrets-in-the-ai-era-navigating-transparency-under-the-eu-ai-act>.

48 European Commission, *supra* note 4.

49 *Who Governs AI in the EU? A Breakdown of Authorities in the EU AI Act*, UNESCO (22 December 2025), <https://www.unesco.org/en/articles/who-governs-ai-eu-breakdown-authorities-eu-ai-act>.

50 Wu Riqiang, *Keeping Pace with the Times: China's Arms Control Tradition, New Challenges, and Nuclear Learning*, 50 Int'l Sec. 82 (2025).

diplomatic complication; it is a structural obstacle to building a liability framework that depends on reciprocal recognition and cross-border enforcement.

IV. *Why Sequencing Matters*

Taken together, these institutional differences suggest that sequencing is essential. Attempting to negotiate or mirror a comprehensive AI liability regime across systems with sharply divergent enforcement cultures and transparency norms risks producing vague commitments, inconsistent enforcement or lowest-common-denominator standards.⁵¹ In practice, that type of approach is unlikely to produce the clear and enforceable governance structure Indiana would need for high-risk AI systems.

A more realistic strategy is phased development. At the international level, this may involve initial coordination among jurisdictions with high institutional capacity, primarily the United States and the EU, followed by gradual expansion once workable cybersecurity and liability baselines are established. At the state level, Indiana should look first to models that combine transparent enforcement, predictable obligations and demonstrated exportability rather than attempting to synthesize incompatible systems.

This sequencing does not permanently exclude other AI powers. Rather, it reflects the reality that durable governance is more likely to emerge if Indiana builds its liability framework on institutions and norms that are already legible, enforceable and credible within its own legal tradition. Indiana already addresses many AI-related risks through existing consumer protection, employment, fraud and data security statutes rather than through a dedicated AI liability framework.⁵² As Indiana practitioners and businesses increasingly recognize, that diffuse approach may address isolated harms, but it does not provide a coherent prospective allocation of responsibility for AI-driven cyber incidents in high-risk sectors.⁵³

In this light, the comparative analysis presented in this part is not merely descriptive. It functions as a filter for determining which elements of foreign and federal AI governance can be productively incorporated into Indiana law and which would introduce more uncertainty than they resolve. The next part applies that filter to propose a targeted Indiana framework for high-risk AI systems, drawing on the most exportable features of the EU and U.S. approaches while avoiding their most significant weaknesses.

51 Alex Whaples, *AI Regulation Across Borders: Legal Challenges and Prospects for International Cooperation*, 26 San Diego Int'l L.J. 317 (2025).

52 Ind. Code § 24-4.9 (Indiana data breach notification statute requiring entities that own or license personal information to disclose security breaches to affected Indiana residents); Ind. Code § 24-15 (Indiana Consumer Data Protection Act establishing consumer data privacy rights and obligations for entities processing personal data of Indiana residents); *Indiana AI Laws You Should Know* (2026), PivIT Strategy (2026), <https://www.pivitstrategy.com/indiana-ai-laws/> [hereinafter *Indiana AI Laws*].

53 *Indiana AI Laws*, *supra* note 52.

D A Targeted Indiana Framework for High-Risk AI Systems

Having identified the liability gaps exposed by AI-driven cyber incidents and examined the comparative approaches of the United States, the EU and China, this part proposes a targeted Indiana framework for high-risk AI systems. The EU and U.S. models serve as comparative reference points of tested governance principles that Indiana can adapt to its own regulatory and economic environment. The purpose of this framework is not to resolve all questions of global AI governance; nor does it intend to impose a comprehensive regulatory regime on artificial intelligence as a whole. Rather, it aims to establish a credible, enforceable model for allocating responsibility and reducing systemic cyber risk in the sectors where Indiana faces the greatest exposure.

I. Why Indiana Needs a Coherent Liability Framework

Indiana currently addresses AI-related harms through a combination of existing consumer protection statutes, employment regulations, fraud laws and data security requirements rather than through a dedicated AI liability framework.⁵⁴ This incremental approach reflects Indiana's historically pragmatic regulatory posture and avoids prematurely imposing broad restrictions on emerging technologies. Yet the same approach also creates fragmentation. AI-driven cyber risks are currently governed through disconnected statutory and regulatory mechanisms that were not designed to allocate responsibility for autonomous or adaptive systems operating across layered digital environments.

As Indiana practitioners increasingly recognize, organizations using AI systems already face meaningful compliance obligations under existing law, particularly in areas involving consumer protection, employment practices, fraud prevention and cybersecurity.⁵⁵ Those obligations, however, remain reactive and diffuse. They may address isolated harms after they occur, but they do not provide a stable prospective framework for allocating liability, establishing cybersecurity expectations or defining governance obligations for high-risk AI systems.

This gap is particularly significant in Indiana because many of the state's core industries, including health care, manufacturing, logistics, finance and energy, face significant cybersecurity risks under rapid technological transformation.⁵⁶ As AI systems become more autonomous and operationally embedded, Indiana's current patchwork approach risks producing uncertainty for businesses, regulators,

⁵⁴ *Id.*

⁵⁵ *Id.*

⁵⁶ *Future Ready: Advancing Indiana's Productivity Through Critical Manufacturing Subsectors*, Conexus Indiana (6 August 2025), <https://conexusindiana.com/blog/2025/08/06/future-ready-advancing-indianas-productivity-through-critical-manufacturing-subsectors/>; *State of Hoosier Cybersecurity 2025*, Ind. Exec. Council on Cybersecurity (January 2025), <https://www.ibrc.indiana.edu/studies/State-of-Hoosier-Cybersecurity-2025.pdf>.

insurers and courts attempting to determine responsibility when AI-driven cyber harms occur.

One objection to state-level action is federal pre-emption. The December 2025 White House executive action on ‘Eliminating State Law Obstruction of National Artificial Intelligence Policy’ signals that the federal executive is attentive to state AI regulation that could fragment national policy.⁵⁷ That pressure is real, but it does not foreclose the framework proposed here. Indiana’s proposal operates through traditional state powers over tort liability, consumer protection and data security—not as a freestanding ‘AI regulation’ of the kind the federal action targets. A narrowly scoped, process-and-disclosure framework focused on high-risk sectors is materially different from a state statute that purports to govern AI development nationally or imposes obligations inconsistent with federal agency guidance. Indiana can therefore proceed on the reasonable assumption that a carefully scoped, sector-specific framework grounded in established state law authority is unlikely to present a pre-emption conflict, while remaining attentive to how federal AI policy develops.

Indiana therefore should not attempt to regulate all AI systems comprehensively. Instead, the state should adopt a targeted, risk-based framework focused specifically on high-risk AI systems whose failure, misuse or compromise could create substantial cybersecurity, operational, financial or public safety consequences. Such a framework would allow Indiana to improve accountability and risk management without unnecessarily restricting innovation or ordinary low-risk AI applications.

II Defining High-Risk AI Systems

At the core of the proposed framework is a clear and predictable allocation of liability. One of the central deficiencies identified in Part B is the ease with which responsibility for AI-related cyber harms can be diffused across developers, deployers and other actors, leaving injured parties without effective remedies. Indiana’s framework should address this problem by distinguishing among these actors while avoiding an overly rigid or punitive liability scheme.

Developers would bear responsibility for negligent design decisions that create foreseeable cyber vulnerabilities, including the failure to address well-documented adversarial techniques or to implement reasonable safeguards consistent with the system’s intended use. Deployers, by contrast, would be liable for misuse, inadequate configuration or deployment of AI systems in environments that exceed their documented risk profile.

This layered allocation of liability ensures that accountability follows control and decision-making authority, while preventing any single actor from externalizing the full cost of AI-driven cyber risk.

Any workable Indiana framework must begin by limiting its scope. Attempting to regulate all AI systems uniformly would likely create excessive compliance burdens while failing to distinguish between low-risk tools and systems capable of causing substantial harm. Indiana should instead adopt a risk-based classification

57 White House, *supra* note 40.

model similar in structure to the EU's AI Act while tailoring that framework to Indiana's regulatory and economic environment.

Under such a framework, 'high-risk AI systems' should include AI technologies deployed in sectors where cyber incidents or operational failures could produce significant legal, financial or public safety consequences. These sectors should include health care, financial services, transportation, utilities, critical infrastructure, election systems and AI systems processing sensitive personal or biometric data. Indiana should also classify systems capable of autonomous cybersecurity operations, including systems capable of network monitoring, automated defensive actions or autonomous system access, as high-risk technologies subject to heightened governance obligations.

At the same time, Indiana should avoid unnecessarily regulating low-risk or consumer-oriented AI systems whose failures are unlikely to create systemic harm. General productivity tools, low-risk generative AI applications and internal business assistance systems should ordinarily remain outside the framework unless deployed in sensitive operational contexts. This narrower scope would reduce compliance burdens while allowing Indiana regulators to focus resources on systems most likely to create significant cyber or operational risk.

A risk-based approach would also provide flexibility as AI technologies evolve. Rather than relying on rigid technical definitions that may quickly become obsolete, Indiana could authorize a designated state agency to periodically update classifications based on evolving technological capability, threat intelligence and industry deployment trends.

III Baseline Cybersecurity Obligations for High-Risk AI

Indiana's framework should impose baseline governance and cybersecurity obligations on developers and deployers of high-risk AI systems. These obligations should focus primarily on process, documentation and risk management rather than imposing strict liability for every AI-related failure. Such an approach would encourage reasonable safeguards while recognizing that no AI system can be made entirely risk-free.

At minimum, developers and deployers of high-risk AI systems should be required to conduct documented risk assessments before deployment. These assessments should evaluate foreseeable cybersecurity risks, adversarial misuse, operational dependencies, training-data integrity concerns and the potential consequences of system failure or manipulation. Organizations should also be required to implement reasonable post-deployment monitoring procedures capable of identifying material changes in system behaviour or emerging vulnerabilities.

Indiana should further require adversarial testing and security validation for high-risk AI systems before deployment into sensitive environments. Because AI systems may be vulnerable to prompt injection, model manipulation, data poisoning or unauthorized autonomous actions, periodic testing should evaluate whether systems can be exploited in ways that create foreseeable cybersecurity or operational harm.

The framework should also require organizations to maintain sufficient documentation regarding system design, deployment conditions, known limitations

and incident history. These records would not only improve organizational accountability but also assist regulators, insurers and courts in evaluating whether reasonable cybersecurity practices were followed in the event of a dispute or incident.

In addition, Indiana should require meaningful human oversight for high-risk AI systems deployed in sensitive operational environments. Human oversight does not require continuous manual supervision of every AI action.⁵⁸ Rather, organizations should ensure that appropriately trained personnel retain authority to monitor system performance, intervene when necessary and suspend autonomous operations where significant risk emerges.

IV Liability Allocation Among Developers and Deployers

One of the primary weaknesses identified in Part B is that existing liability doctrines struggle to distinguish responsibility among the multiple actors involved in AI deployment. Indiana's framework should therefore clarify baseline responsibility for both developers and deployers of high-risk AI systems.

Developers should remain responsible for harms arising from negligent design, inadequate safeguards, foreseeable misuse or material failures to disclose known system limitations. Where a developer fails to implement reasonable cybersecurity protections, ignores foreseeable adversarial vulnerabilities or materially misrepresents system capabilities, liability should remain available under Indiana law.

Deployers, however, should not be permitted to avoid responsibility simply because a third-party AI model was involved. Organizations implementing high-risk AI systems should remain responsible for negligent deployment, unsafe operational integration, improper configuration or failures to respond appropriately to known system risks. In practice, many AI-related harms may result not from the underlying model itself but from the manner in which organizations implement, monitor or operationalize those systems within sensitive environments.⁵⁹

Indiana should also recognize that liability allocation in AI systems may require shared responsibility rather than exclusive fault assignment. In some cases, both developers and deployers may contribute materially to an AI-driven cyber incident. A framework recognizing comparative allocation principles would more accurately reflect the layered nature of modern AI deployment ecosystems.

V Safe Harbours and Incentive Alignment

Indiana's framework should avoid discouraging beneficial innovation by imposing unrealistic or punitive liability standards. Organizations acting in good faith to comply with recognized governance and cybersecurity obligations should receive meaningful legal incentives for responsible conduct.

58 *Human Oversight of AI Systems*, NewTech.Law, <https://newtech.law/en/articles/human-oversight-of-ai-systems> (last visited 22 May 2026).

59 Mia Hoffmann, *The Mechanisms of AI Harm: Lessons Learned from AI Incidents*, Ctr. for Sec. & Emerging Tech. (October 2025), <https://cset.georgetown.edu/publication/the-mechanisms-of-ai-harm-lessons-learned-from-ai-incidents/>.

One approach would be to create rebuttable presumptions of reasonable care for organizations that substantially comply with approved AI governance standards, documented risk assessment procedures and recognized cybersecurity frameworks. Similar safe-harbour approaches already exist in other areas of cybersecurity and privacy regulation and may encourage organizations to adopt stronger governance practices proactively rather than defensively after litigation arises.⁶⁰

Indiana could also encourage innovation through regulatory sandbox programmes or limited pilot-authority mechanisms allowing organizations to test emerging AI systems under supervised conditions. Such programmes would permit experimentation while still preserving oversight and risk-management expectations for systems deployed in sensitive sectors.

Importantly, safe-harbour protections should not apply where organizations intentionally disregard known risks, conceal material vulnerabilities or deploy high-risk AI systems without reasonable governance safeguards. The purpose of Indiana's framework should not be to immunize AI deployment from liability but, instead, to encourage responsible implementation while reducing uncertainty for organizations attempting to comply in good faith.

VI *Incident Reporting and Coordinated Response*

Indiana should also incorporate targeted incident reporting obligations for significant AI-driven cybersecurity events involving high-risk systems. Current breach notification laws focus primarily on compromised personal information, but AI-related incidents may create operational, infrastructure or public safety harms even where traditional data breaches do not occur.⁶¹

Under Indiana's framework, organizations deploying high-risk AI systems should report material AI-related cybersecurity incidents to designated state authorities within a reasonable period after discovery. Reporting requirements should apply primarily to incidents involving substantial operational disruption, unauthorized autonomous system behaviour, critical infrastructure interference or significant compromise of sensitive systems or data.

Indiana should also encourage information-sharing mechanisms between state agencies, critical infrastructure operators and private sector organizations. Because AI-related threats evolve rapidly, coordinated reporting and threat intelligence sharing may improve both public and private cybersecurity resilience.

VII *Why Indiana Is Well Positioned to Act*

Indiana is well positioned to act precisely because the comparative analysis in Part C identifies what effective AI governance requires—transparent enforcement, predictable obligations and adaptable standards—and Indiana's existing legal

60 Joe Köller, *US Cybersecurity Safe Harbor Laws by State: All Current Legislation*, Tenfold Security (12 March 2025), <https://www.tenfold-security.com/en/cybersecurity-safe-harbor-laws/>.

61 Avinash Agarwal & Manisha J. Nene, *Incorporating AI Incident Reporting into Telecommunications Law and Policy: Insights from India*, arXiv (2025), <https://arxiv.org/pdf/2509.09508>.

institutions already satisfy those baseline conditions. Indiana operates within a rule-of-law system that provides judicial review, agency accountability and stable enforcement mechanisms. A targeted Indiana framework can therefore draw credibly on the governance principles that make EU and U.S. approaches workable, without attempting to replicate the scale or scope of either.

Indiana can adopt a narrower and more operationally focused framework than broader international models while still incorporating many of the most effective governance principles emerging from the EU and federal guidance. Rather than attempting to become a comprehensive AI regulator, Indiana can focus specifically on high-risk operational systems where AI-driven cyber incidents are most likely to produce substantial harm.

A targeted Indiana framework would therefore serve two functions simultaneously. First, it would provide businesses, courts, insurers and regulators with clearer expectations regarding cybersecurity governance and liability allocation for high-risk AI systems. Second, it would position Indiana as a state capable of addressing emerging AI risks pragmatically without abandoning flexibility, innovation or economic competitiveness.

E Conclusion

Artificial intelligence has altered the cybersecurity landscape in ways that existing liability frameworks were not designed to accommodate. As AI systems become increasingly autonomous, adaptive and operationally embedded within critical infrastructure, traditional doctrines of product liability, negligence and contract law struggle to assign responsibility when AI-driven cyber harms occur. The result is not merely doctrinal uncertainty but a growing accountability gap in which developers, deployers and other actors can diffuse responsibility while operational and cybersecurity risks continue to expand.

Indiana's current approach reflects the broader fragmentation of AI governance in the United States. Existing consumer protection statutes, data security obligations, fraud laws and sector-specific regulations address portions of AI-related risk, but they do so indirectly and without a coherent framework for allocating responsibility in high-risk environments. As Indiana industries increasingly integrate AI into health care systems, logistics networks, manufacturing operations, financial services and cybersecurity infrastructure, that fragmented approach becomes increasingly difficult to sustain.

This article has argued that Indiana should adopt a targeted, risk-based liability and cybersecurity framework focused specifically on high-risk AI systems. Drawing selectively from the clearer accountability structures emerging in the EU while preserving the flexibility traditionally associated with the American regulatory approach, Indiana can establish more predictable governance obligations without unnecessarily restricting innovation. Such a framework would improve cybersecurity resilience, clarify liability allocation among developers and deployers

and create stronger incentives for organizations to adopt meaningful governance and risk-management practices before harm occurs.

Importantly, the proposed framework does not attempt to regulate all AI systems comprehensively. Instead, it recognizes that the greatest governance concerns arise where AI systems operate in sensitive or high-impact environments capable of producing significant operational, financial or public safety consequences. By focusing on high-risk systems, Indiana can adopt a narrower and more practical framework that remains adaptable as technologies evolve.

The comparative analysis in this article also demonstrates that institutional capacity matters as much as substantive regulation. Effective AI governance requires more than the existence of formal rules. It depends on transparent enforcement, procedural reliability and the ability to translate technical standards into meaningful legal accountability. In that respect, the United States and the EU provide more workable models for Indiana than systems characterized by opaque enforcement or broad state discretion.

The comparison also carries lessons in the other direction. The EU's process-based AI Act model offers clearer prospective accountability than the U.S. approach, but the American experience with flexible, sector-specific liability frameworks suggests that overly prescriptive mandates risk becoming brittle as AI capabilities evolve faster than regulatory cycles. For European policymakers, the U.S. model's tolerance for after-the-fact litigation is a warning about accountability gaps, but its preservation of adaptive flexibility is a design feature worth weighing as the EU considers how its own framework performs against rapidly changing threat environments.

Ultimately, the problem posed by AI-driven cyber incidents is not simply technological, but institutional. Existing legal frameworks were developed for human-directed systems operating within more predictable chains of causation and responsibility. AI systems increasingly challenge those assumptions. If Indiana continues relying exclusively on fragmented and reactive approaches, accountability gaps will likely widen as AI capabilities become more deeply integrated into critical infrastructure and operational decision-making. A targeted Indiana framework for high-risk AI systems therefore represents not an attempt to halt innovation but, instead, an effort to ensure that innovation develops alongside meaningful responsibility, cybersecurity resilience and public trust.