Draft date: 11/10/26

2026 Fall National Meeting
Dallas, Texas

INNOVATION, CYBERSECURITY, AND TECHNOLOGY (H) COMMITTEE
Tuesday, November 17, 2026
12:15 – 1:30 p.m.
Convention Center—Texas AB—Level 3

ROLL CALL

Michael Yaworsky, Chair	Florida	Angela L. Nelson	Missouri
Karima M. Woods, Vice Chair	District of Columbia	James E. Brown	Montana
Mark Fowler	Alabama	Eric Dunning	Nebraska
Heather Carpenter	Alaska	Jon Godfread	North Dakota
Jimmy Harris	Arkansas	Michael Humphreys	Pennsylvania
Michael Conway	Colorado	Carter Lawrence	Tennessee
Doug Ommen	Iowa	Kaj Samsom	Vermont
Marie Grant	Maryland		

NAIC Committee Support: Miguel Romero/Scott Morris/Scott Sobel

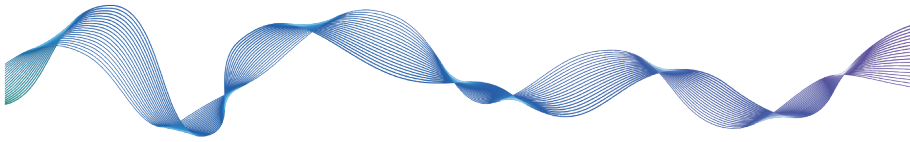
AGENDA

1. Consider Adoption of its April 30 and Summer National Meeting Minutes—*Commissioner Karima Woods (DC)* — Attachment One

2. Consider Adoption of the Reports of its Working Groups—*Commissioner Karima Woods (DC)* — Attachment Two
   A. Big Data and Artificial Intelligence (H) Working Group
   B. Cybersecurity (H) Working Group
   C. Privacy Protections (H) Working Group
   D. SupTech/GovTech (H) Subgroup
   E. Third-Party Data and Model (H) Working Group

3. Consider Adoption of the AI Risk Evaluation Supplement —*Commissioner Michael Yaworsky (FL)* — Attachment Three

4. Consider Adoption of its 2027 Proposed Charges —*Commissioner Michael Yaworsky (FL)* — Attachment Four



5. Hear a Presentation on How the Audit Profession is Adapting for Artificial Intelligence (AI)—*Michelle Donahue (Deloitte)* — Attachment Five

6. Discuss Any Other Matters Brought Before the Committee —*Commissioner Michael Yaworsky (FL)*

7. Adjournment

Draft Pending Adoption

Draft: 8/27/26

Innovation, Cybersecurity, and Technology (H) Committee
Columbus, Ohio
August 14, 2026

The Innovation, Cybersecurity, and Technology (H) Committee met in Columbus, OH, August 14, 2026. The following Committee members participated: Michael Yaworsky, Chair (FL); Heather Carpenter (AK); Mark Fowler (AL); Jimmy Harris (AR); Michael Conway and Jason Lapham (CO); Doug Ommen and Daniel Mathis (IA); Marie Grant (MD); James E. Brown represented by Erin Snyder (MT); Jon Godfread (ND); Eric Dunning (NE); Michael Humphreys represented by Jodi Frantz and Michael McKenney (PA); Carter Lawrence represented by Scott McAnally (TN); and Kaj Samsom and Mary Block (VT). Also participating were: Joshua Hershman and George Bradner (CT); Judith L. French (OH); Glen Mulready (OK); Elizabeth Kelleher Dwyer and Matthew Gendron (RI); Amanda Crawford and Marianne Baker (TX); Jon Pike (UT); and Scott A. White, Eric Lowe, and Michael Peterson (VA).

1. Adopted the Reports of its Working Groups and Subgroup

A. Big Data and Artificial Intelligence (H) Working Group

Block reported that the Big Data and Artificial Intelligence (H) Working Group met Aug. 13. During that meeting, the Working Group adopted its July 22 minutes. The Working Group then received an update on the Artificial Intelligence Risk Evaluation Supplement (AIRES) pilot process. The pilot, which began in March, involves 12 participating states and will continue through September. Through the pilot, states are learning about the use of artificial intelligence (AI) while providing feedback that will help clarify many aspects of the supplement. The next version of the supplement will be shared at the end of August, followed by two rounds of public exposure. Public updates will be provided throughout the pilot process, with the goal of adopting the supplement at the Fall National Meeting.

The Working Group closed its meeting by hearing a presentation from Edin Imsirovic (AM Best) on AI governance in insurance. The presentation defined predictive AI, generative AI, and agentic AI; described innovation and enterprise risk management (ERM) perspectives for evaluating governance quality and how governance can affect value and risk; and discussed the inputs, outputs, and control challenges across AI capability tiers.

B. Cybersecurity (H) Working Group

Peterson reported that the Cybersecurity (H) Working Group met June 2 in regulator-to-regulator session, pursuant to paragraph xx (insert appropriate text) of the NAIC Policy Statement on Open Meetings, to demonstrate the proposed cybersecurity event notification portal. Kim Myers (NAIC) demonstrated a nonfunctional prototype to illustrate the tool's intended capabilities across both an industry licensee interface and a regulator interface. The tool supports structured question-and-answer workflows at the event level, with resolution tracking, reminders, and exportable records comparable to existing Uniform Certificate of Authority Application (UCAA) functionality. The portal proposal has been reviewed and approved at the Working Group, Committee, and Enterprise Project Management Office (EPMO) levels, and the next step is for the Executive (EX) Committee to review and approve it.

The Working Group then met June 10 and heard a presentation on the NetDiligence 2025 *Cyber Claims Study*. The study draws on a five-year data set of about 10,400 claims focused primarily on small- and mid-sized enterprises (SMEs). According to the study, the average SME incident cost was approximately $203,000 in 2024, compared with approximately $5 million for large entities. Ransomware was cited as a leading peril and the top driver of

© 2026 National Association of Insurance Commissioners

demand, with SME demands averaging $3.1 million and then negotiated down to about $1 million. A notable shift from prior years was that nearly all 2024 claims were tied to criminal activity, with business email compromise identified as the second-leading cause of loss, typically involving automated clearing house (ACH) or wire fraud through executive impersonation. In discussion, the Working Group explored the data elements needed to move from tracking claim volume toward understanding incident impacts and the frequent inadequacy of purchased coverage limits relative to actual incident costs. The Working Group is looking to coordinate multiple interim meetings in the coming months to hear about and discuss the emerging risks around quantum computing and post-quantum cryptography, as well as the impact of frontier AI models on the cybersecurity landscape.

C. Privacy Protections (H) Working Group

Director Dwyer reported that the Privacy Protections Drafting Group met June 3 and April 30 to consider changes to Article 7 and Article 8 of the *Privacy of Consumer Financial and Health Information Regulation* (#672).

On July 24 the Working Group exposed the full draft of Model #672, incorporating all of the work completed on the individual sections, for a 60-day public comment period ending Sept. 22.

The Working Group also Aug. 13 to hear verbal comments on the full draft of the revised Model #672. Once the written comments are received, the Working Group will compile and review them. After the chairs review the comments, the Working Group will communicate its next steps, which will depend on the comments received.

D. SupTech/GovTech (H) Subgroup

Bradner reported that the SupTech/GovTech (H) Subgroup focuses on regulatory tools and education and hears from companies on their proprietary technology. Its meetings are conducted in regulator-to-regulator session following the NAIC Policy Statement on Open Meetings.

The Subgroup continues to use the results of a regulator survey conducted last year to identify topics that drive efficiency, reduce administrative burden, and strengthen regulatory effectiveness. Since the Spring National Meeting, the Subgroup met twice. On May 27, it convened state insurance regulators to exchange ideas on how insurance departments are approaching AI adoption and the use of AI tools in insurance regulation, including practical lessons learned, challenges, and open questions. On July 28, the Subgroup viewed a demonstration of Deloitte's resiliency navigator system, a consumer-facing platform that helps state departments of insurance (DOIs) close the consumer education gap before and after a loss. The Subgroup continues to evaluate additional presentations and educational opportunities for 2026 on technical topics that would benefit regulators' collective understanding and improve efficiency and oversight capabilities.

E. Third-Party Data and Models (H) Working Group

Lapham reported that the Third-Party Data and Models (H) Working Group met Aug. 12. During that meeting, the Working Group adopted its July 16 and Spring National Meeting minutes and heard comments on the exposed draft third-party regulatory framework for property/casualty (P/C) pricing and underwriting. He said that Working Group received 11 comment letters from interested parties on the exposed draft framework. The general themes of the comments included: 1) concerns with the attestation asking vendors to certify compliance they cannot control; 2) inadequate and uncertain confidentiality protections for vendor filings across states; 3) whether registration would be voluntary given the consequences of use restrictions; 4) the need to define material change objectively; and 5) duplication of existing state filing and oversight processes. The drafting group will meet soon to weigh revisions to the draft framework based on this recent feedback for consideration by the full Working Group, with the hope that the framework will be ready for potential adoption at the Fall National Meeting.

Additionally, it was reported that the Committee met April 30 (Attachment One). During this meeting, it took the following action: 1) adopted its Spring National Meeting minutes (*see NAIC Proceedings – Spring 2026, Innovation, Cybersecurity, and Technology (H) Committee*); and 2) adopted the cybersecurity event notification portal project proposal.

Commissioner Carpenter made a motion, seconded by Commissioner Conway, to adopt the reports of the: Big Data and Artificial Intelligence (H) Working Group (Attachment Two), including its July 22 and June 1 minutes; Cybersecurity (H) Working Group (Attachment Three), including its June 10 minutes; Privacy Protections (H) Working Group (Attachment Four); Third-Party Data and Models (H) Working Group (Attachment Five), including its Feb. 26 minutes; SupTech/GovTech (H) Working Group; and Data Call Study Group. The motion passed unanimously.

2. Heard a Presentation from Microsoft on AI Trends in the Insurance Industry

The Committee heard a presentation from Microsoft on AI trends in the insurance industry. Jim DeMarco (Microsoft), an insurance advisor lead, outlined four broad trends reshaping the industry.

DeMarco first pointed to automation, noting that the first insurance claim processed solely by AI occurred in 2023—a stolen-bicycle claim in the United Kingdom (UK) that took two seconds to process. He next described a shift in distribution, observing that the first policy offered, bound, and sold entirely through ChatGPT occurred earlier this year in Spain, after which the small insurer that offered the policy, Twee O, was acquired by a larger competitor. Third, he addressed demographic change, citing reporting on a study suggesting a maximum human age of 194 years and noting that people are living longer but not necessarily healthier, with implications for wellness, elder care, financial risk transfer, and the broader wealth transfer. Fourth, he discussed weather and weather modeling, noting that severe convective storms are becoming more frequent and severe, that Tornado Alley has shifted east. He said that AI is improving both longer-range forecasting and imminent-risk identification, creating opportunities for risk mitigation and prevention services that lower the cost of loss. DeMarco said these trends are changing the fundamental assumptions underlying how the industry views risk, risk transfer, and claims payment.

Turning to the use of AI in the insurance industry, DeMarco focused on agentic AI—the granting of agency to predictive models to make decisions—which he said could transform underwriting, claims, and distribution. However, he cautioned that AI is a tool rather than an inherently intelligent system and must be adapted to the appropriate use case. He said large language models (LLMs) from various providers are not themselves a differentiator. Rather, the differentiator is how they are used, and a tool that improves remains ineffective in the hands of someone using it poorly. He said AI is changing jobs rather than eliminating the need for human workers, using the analogy that stronger hurricane-modeling tools narrow predicted storm paths but do not remove the need for catastrophe modelers. On scaling, DeMarco cited a Boston Consulting Group report ranking insurance second only to the technology industry in AI use but near the bottom in scaling that use, observing that the industry tends to experiment and leave capabilities in isolated pockets. He said scaling AI across an organization requires systemic governance that brings intelligence to the point of decision while ensuring its use is trustworthy.

DeMarco organized current use cases into four categories. He described as proven, or table stakes: 1) the use of compliant grounded search with natural language processing and generative AI to reduce response times from days to seconds; 2) contextualized document processing; 3) guidance to professionals in claims and underwriting, including underwriter-assistance tools that are more mature outside the U.S.; and 4) assistance for brokers, agents, and call-center interactions.

In terms of what works, DeMarco said the greatest current energy is in guiding customer interactions and in straight-through processing for underwriting, while similar automation for claims is advancing but not fully realized, particularly for adverse decisions. For those decisions, DeMarco said Microsoft advocates keeping humans in the loop. He cited the analogy that although autopilot has existed for flight and landing since 1947 and for takeoff since 2024, passengers still want a pilot on board. Predictive AI is very good at determining what could happen next, but it is not suited to deciding what should happen.

Among promising developments, DeMarco pointed to tools that emulate a person at a keyboard to work with legacy mainframe systems, tools that identify new data to test actuarial assumptions, and tools that automate risk mitigation, such as increasingly precise alerts warning policyholders of approaching hailstorms.

DeMarco said AI is not ready to provide judgment, because predictive AI—including generative and agentic AI—lacks abductive reasoning, so human-level decision-making remains necessary.

On governance, DeMarco said that scaling AI immediately raises governance questions and that financial institutions, including insurers, must govern their entire interconnected ecosystems and data—both their own and data received from others—rather than individual models alone. He noted the systemic risk that governance itself can pose, citing the example of a model that could no longer be exported outside the U.S., and said oversight must occur at the organizational level. He described a framework for trust that is both architectural and systemic, in which AI agents have identities, are restricted in what they can access as any employee would be, and can explain what they have done and how they used data, supported by a responsible AI framework. He concluded that AI is increasingly providing intelligence at the point of decision and that failing to manage trust would provoke backlash from the public and customers alike.

Following the presentation, Commissioner Yaworsky described a scenario in which a health insurer compared its usual human-involved claims process with a nearly fully automated AI process that produced more accurate and better outcomes. However, he said most participants in his discussions still preferred substantial human involvement even when outcomes were poorer, reflecting a desire for humanity and trust in the process. DeMarco responded that an auto insurer that shifted first notice of loss to AI achieved strong call-deflection rates and responsiveness, but 35% of customers immediately requested a representative because people under stress want to speak with people. He noted that studies indicate that human decision-makers tend to reach better outcomes earlier in the day than later. He said the key question is the right outcome for the claimant—such as getting a car back on the road or access to a medication—rather than merely processing a claim, adding that simply digitizing an existing human process is unlikely to improve outcomes.

Miguel Romero (NAIC) said that state insurance regulators had heard in a prior session about the growing use of AI to generate consumer complaints, which can make it harder to identify the underlying issue and verify the facts. He asked whether solutions could help consumers advocate for themselves without creating additional workload for companies or regulators. DeMarco said that every tool can be used as a weapon and that some bad actors may be using AI to submit high volumes of complaints. He drew a parallel to the evolution of social media and to cybersecurity, where AI is used by criminals and state-sponsored actors, and the response must likewise incorporate AI to predict, identify, and respond. He said insurance departments will likely need tools to distinguish genuine complaints from fabricated ones and then respond appropriately—human-to-human contact when needed, human-to-technology contact for information seeking, and technology-to-technology filtering for spam. DeMarco said he anticipates the increasing use of personalized agents that will, over time, communicate with regulators and insurers on consumers' behalf.

© 2026 National Association of Insurance Commissioners

3. Received an Update on the Cybersecurity Event Notification Portal

Commissioner Yaworsky provided an update on the cybersecurity event notification portal. He noted that the NAIC had experienced a cybersecurity event several weeks earlier and said the purpose of the discussion was not to review that event but to acknowledge and address concerns raised afterward about the NAIC creating a portal and the data that would be housed within it.

Commissioner Yaworsky recalled that the proposal to adopt the portal project had been adopted at the Spring National Meeting. Before the project is considered by the NAIC's Executive (EX) Committee, he asked NAIC committee support to work with Commissioner Crawford to perform a security review of the project, noting that her background in technology would help ensure the membership could move forward responsibly. He said this was a novel situation without a predefined scope for the review, but he expressed confidence in Commissioner Crawford's ability to guide the effort. He suggested that one component could be a clear, easy-to-read listing of the security commitments the NAIC provides to its membership and regulated entities so everyone could understand the safeguards in place for data housed in the portal. He said much of this had already been discussed during the portal's development and expressed hope that the review would be brief. Commissioner Yaworsky invited questions or comments, and none were raised.

4. Discussed Other Matters

Director Dunning announced that Commissioner Crawford, Commissioner Godfread, Commissioner Yaworsky, and Director Dwyer are scheduled to speak Oct. 20 at Insurtech on the Silicon Prairie, which will be held Oct. 20–21 in Omaha, NE. Having no further business, the Innovation, Cybersecurity, and Technology (H) Committee adjourned.

SharePoint/NAIC Support Staff Hub/Committees/H CMTE/2026_Summer/H-Minutes/Minutes-H-Cmte081426-Final.docx

© 2026 National Association of Insurance Commissioners

Draft Pending Adoption

Attachment One
Innovation, Cybersecurity, and Technology (H) Committee
8/14/26

Draft: 8/27/26

Innovation, Cybersecurity, and Technology (H) Committee
Virtual Meeting
April 30, 2026

The Innovation, Cybersecurity, and Technology (H) Committee met virtually on April 30, 2026. The following Committee members participated: Michael Yaworsky, Chair (FL); Karima M. Woods, Vice-Chair (DC); Heather Carpenter and Molly Nollette (AK); Mark Fowler represented by Richard Fiore (AL); Jimmy Harris represented by Chris Erwin (AR); Michael Conway represented by Jason Lapham (CO); Doug Ommen (IA); Marie Grant (MD); Angela Nelson (MO); Jon Godfread represented by Colton Schulz (ND); Eric Dunning (NE); Carter Lawrence (TN); and Mary Block and Jared Holshouser (VT). Also participating were: Scott A. White and Michael Peterson (VA)

1. Adopted its 2026 Spring National Meeting Minutes

Schulz made a motion, seconded by Commissioner Lawrence, to adopt the Committee's March 25, 2026, minutes (*see NAIC Proceedings – Spring 2026, Innovation, Cybersecurity, and Technology (H) Committee*). The motion passed unanimously.

2. Adopted the Cybersecurity Event Notification Portal Project Proposal

The Committee next considered the Cybersecurity Event Notification Portal Project Proposal. Commissioner Yaworsky noted the portal would allow states to receive cybersecurity event notices through an NAIC-developed application, simplify compliance burdens, enhance the security of notification information, and leverage the NAIC's capacity to develop in-house applications tailored to regulator input. The Chair stated the proposal had been discussed extensively at both the Committee and working group levels and that the Cybersecurity (H) Working Group adopted the project proposal at its March 13, 2026, meeting.

Peterson provided an overview of the project. Peterson described the project's origin following the adoption of the *Insurance Data Security Model Law* (#668) and the Cybersecurity Event Response Plan. He explained that at the 2024 Fall National Meeting, the NAIC adopted a motion directing NAIC committee support to explore the creation of the portal. In 2025, NAIC committee support developed detailed project documentation, which underwent multiple rounds of public comment from both regulators and industry. Following the incorporation of those comments, the project documentation reached a stable consensus and was adopted by the Working Group in March 2026.

Peterson stated the portal is intended to address fragmentation in cybersecurity event notification requirements across the 28 jurisdictions that have passed versions of Section 6(B) of Model #668. He noted the portal is designed to centralize and standardize the notification process by providing a single standardized form that captures all jurisdictional variations. He stated this approach would reduce current and future compliance costs for licensees. Peterson further noted that for states that have not yet adopted the model law, the availability of the portal could serve as an incentive, because adopting the law in conjunction with the portal would effectively reduce rather than increase regulatory burden on licensees. Peterson described the confidentiality and security features of the portal, noting that the NAIC agreed to provide a Service Organization Control (SOC) 3 report to the industry as an assurance mechanism on the NAIC's security.

© 2026 National Association of Insurance Commissioners

Draft Pending Adoption

Yaworsky provided contextual remarks, referencing prior large-scale cybersecurity breaches affecting the health industry and the challenges regulators faced coordinating responses across jurisdictions without a unified notification system. The Chair stated that a unified portal would significantly improve regulators' ability to assess severity and take timely action. He commended Peterson and the working group for navigating a technically complex and lengthy process.

Commissioner Grant made a motion, seconded by Lawrence, to adopt the Cybersecurity Event Notification Portal Project Proposal (Attachment One-A). The motion passed unanimously. The Chair stated the proposal would be forwarded to the NAIC Executive Committee for consideration.

Having no further discussion, the Innovation, Cybersecurity, and Technology (H) Committee adjourned.

SharePoint/NAIC Support Staff Hub/Committees/H CMTE/2026_Summer/2026 0430Interim-Meeting/Minutes-H-Cmte043026-Final.docx

© 2026 National Association of Insurance Commissioners

Draft: 11/3/26

Cybersecurity (H) Working Group
Virtual Meeting
October 14, 2026

The Cybersecurity (H) Working Group of the Innovation, Cybersecurity, and Technology (H) Committee met Oct. 14, 2026. The following Working Group members participated: Michael Peterson, Chair (VA); Colton Schulz, Vice Chair (ND); Alex Romero and Julia Jette (AK); Chris Erwin (AR); Lori Dreaver Munn (AZ); Damon Diederich (CA); Wanchin Chou, George Bradner, and Kurt Swan (CT); Tim Li (DE); Matt Kilgallen and Paula Shamburger (GA); Daniel Mathis (IA); Nina Hunter (LA); Mary Kwei (MD); Danielle Torres (MI); Gregory Maus and Bubba Aguirre (MN); Troy Smith (MT); Jessica Price (NC); Martin Swanson (NE); Joshua Hilliard (NH); Gille Ann Rabbin (NY); John Pollack and Matt Walsh (OH); Curt Kwak (WA); Jamie Adams and Barbara Belling (WI); and Lela D. Ladd (WY). Also participating were Shannon Hohl (ID); Sandra Darby (ME); Brian Fjeldheim and John Haworth (OR); Matt Gendron (RI); and Tony Dorschner (SD).

1. Heard a Presentation on the Frontier AI Security Readiness and the CrowdStrike Whitepaper

Peterson introduced Brandon Wales (CrowdStrike), noting that Wales leads government affairs and policy engagement across the U.S., Canada, and Latin America and has more than 25 years of national security and cybersecurity experience. Peterson said the presentation would address how artificial intelligence (AI) is changing the speed and economics of cyber risk, shortening the vulnerability life cycle, and creating a new attack surface. Wales presented CrowdStrike's five-step frontier AI security readiness framework.

Wales said AI has not made existing cybersecurity controls obsolete. Instead, it has compressed the time available to identify, assess, and respond to threats. He cited CrowdStrike research showing an 89% year-over-year increase in AI-enabled attacks, a 42% increase in zero-day vulnerabilities exploited before public disclosure, an average e-crime breakout time of 29 minutes, and a fastest observed breakout time of 27 seconds. He asked whether periodic scanning, quarterly assessments, lengthy vulnerability triage, and annual exercises remain appropriate for a machine-speed threat environment.

Wales described a collapsing vulnerability life cycle. He said frontier AI models can analyze large code bases and identify vulnerabilities at a scale that can overwhelm traditional patch-management processes. CrowdStrike identified more than 2,400 potential vulnerabilities across 43 products in one AI-driven research effort. Wales recommended moving beyond vulnerability counts and patching service-level agreements toward continuous identification and reduction of exposures that could cause material harm. He said organizations should connect technical weaknesses to critical systems and business functions and validate whether an adversary could turn an exposure into an incident.

Wales cautioned that frontier AI risk is not solely a vulnerability-management issue. He said adversaries often prefer stolen credentials because legitimate access can be harder to detect and can support follow-on activity. He also described cross-domain attacks, which can exploit fragmented visibility and disconnected security products. Organizations should be able to detect and respond across complex attack life cycles rather than treating individual vulnerabilities as the primary measure of readiness. Wales outlined five elements of the frontier AI security readiness framework:

- **Prioritize by exploitability.** Organizations should focus first on weaknesses that are most likely to be exploited and could produce material harm.

© 2026 National Association of Insurance Commissioners

- **Continuously validate exposure.** Organizations should assess changing network weaknesses on an ongoing basis rather than at a single point in time.
- **Enforce strong identity controls.** Organizations should address human, machine, and AI-agent identities and the trust relationships built into their networks.
- **Detect and respond at machine speed.** Organizations need technology, processes, and personnel capable of responding in real time. Wales said a 27-second breakout cannot be addressed through manual alert triage alone.
- **Apply AI deliberately and securely.** Organizations should secure AI at deployment and maintain visibility into sanctioned and unsanctioned AI, agent behavior, data movement, and malicious activity.

Wales said AI has become an attack surface rather than only a tool. He described risks from malicious code packages, adversaries' use of an organization's AI systems after gaining access to a network, unsanctioned AI, autonomous agent activity, and sensitive data moving into or out of systems. He said governance is necessary but must be supported by technical guardrails. He also characterized AI detection and response technology as available but developing.

Wales compared the current deployment of AI security controls to the federal government's adoption of endpoint detection and response after the SolarWinds incident. He said organizations have deployed AI rapidly without always implementing technology to monitor and secure it. He noted that the National Institute of Standards and Technology (NIST) AI Risk Management Framework is a useful starting point but does not yet have the same body of detailed controls that supports the NIST Cybersecurity Framework.

Wales also discussed AI's defensive benefits. He said cybersecurity tools have incorporated statistical analysis and machine learning for years, helping the industry integrate newer AI capabilities. He identified two promising applications: AI-assisted security operations that triage and act on more alerts and adversarial co-evolution that trains offensive and defensive models together to identify weaknesses and improve defenses. Wales said regulatory programs should recognize defensive AI as an important component of security programs operating at machine speed.

Wales said advanced defensive capabilities should be broadly accessible. Smaller entities may receive these benefits through managed security service providers (MSSPs), managed detection and response (MDR) services, and improvements embedded in underlying technologies. He said the insurance industry can influence cybersecurity practices across many sectors through due diligence, risk analysis, underwriting, and pricing.

Schulz asked what insurance departments should review when insurers use AI coding tools for internal application development. Wales recommended documented governance, monitoring of what tools download and transmit, and supply-chain risk-management practices comparable to those used for external providers. He also recommended using AI to test AI-generated applications for weaknesses and documenting how autonomous tools operate, including the identities and permissions assigned to them. Wales said communities of regulators can help establish common minimum expectations and promote effective practices.

Kilgallen asked whether the NIST AI Risk Management Framework is a sufficient framework to follow. Wales said the framework remains under development and needs more detailed controls to support practical implementation. He said organizations should use it to guide initial risk-management decisions while recognizing that they may need to go beyond it in areas where controls are not yet mature. Debra Decker (Stimson Center) also asked when an update to the framework would be published. Wales said he did not know when the update would be published.

© 2026 National Association of Insurance Commissioners

Hunter asked for minimum expectations that could apply to insurers of different sizes and levels of sophistication. Wales recommended two baseline questions. First, regulators should ask whether an insurer has a documented policy for managing AI and follows it. Second, regulators should ask whether the insurer has deployed technology to monitor and secure the AI it uses. He said organizations cannot credibly claim to use AI securely if they cannot observe its activity, block malicious behavior, and respond to risks.

Wales said small businesses without full-time cybersecurity programs should use an MSSP or MDR service. He said adversaries target internet-accessible weaknesses regardless of an organization's size. Wales also discussed cyber insurers that combine coverage with monitoring, scanning, or MDR services. He said this model can improve security for smaller policyholders and increase insurers' visibility into risk.

Decker discussed whether lenders could encourage or require small and medium-sized business borrowers to obtain cyber insurance. She said cyber insurance underwriting can promote stronger security practices and enable faster adaptation than regulatory requirements. Wales said cyber insurance and managed security services are important risk-management tools for small businesses. He noted that lender requirements could become more likely if cyber incidents produce significant loan losses.

Bradner said Small Business Administration loan programs may provide one avenue for considering cyber insurance requirements. He also identified affordability, availability, and policyholder education as important considerations. He compared the issue to consumer misunderstandings about whether homeowners insurance covers flood losses and said some businesses may similarly assume that commercial insurance includes cyber coverage.

Peterson asked how analysts and examiners should assess both security for AI and AI used for security. Wales said governance and technology should be reviewed together because technology without governance may be directed toward the wrong risks, while governance without technology may not operate at the speed required. He recommended assessing how companies deploy AI to achieve business outcomes, incorporate security into deployment decisions, use AI within security operations, and obtain capabilities through third-party MSSPs or MDR providers. Wales said smaller entities may require more education about the questions they should ask their service providers.

Bradner asked whether the current cybersecurity processes address AI-related risks. Wales said traditional cybersecurity principles and controls remain relevant because AI-enabled attacks still rely on detectable actions, such as credential theft, process execution, and data access. However, organizations may need enhanced capabilities to address increased speed and scale and to secure new attack vectors created by AI deployment.

2. Discussed Other Matters

Peterson said the Working Group's next meeting would include a presentation on the 2025 Cybersecurity Insurance Coverage Supplement data and new ThoughtSpot developments that support regulators' access to annual cyber supplement data. He invited members to submit topics for future Working Group consideration.

Having no further business, the Cybersecurity (H) Working Group adjourned.

© 2026 National Association of Insurance Commissioners

Draft 10/26/2026
Adopted by the Executive (EX) Committee and Plenary, Pending, 2026
Adopted by the Innovation, Cybersecurity, and Technology (H) Committee, Pending, 2026

2026 Proposed Charges

INNOVATION, CYBERSECURITY, AND TECHNOLOGY (H) COMMITTEE

The mission of the Innovation, Cybersecurity, and Technology (H) Committee is to: 1) provide a forum for state insurance regulators to learn about and have discussions regarding: cybersecurity, innovation, data security and privacy protections, and emerging technology issues; 2) monitor developments in these areas that affect the state insurance regulatory framework; 3) maintain an understanding of evolving practices and use of innovation technologies by insurers and producers in respective lines of business; 4) coordinate NAIC efforts regarding innovation, cybersecurity and privacy, and technology across other committees; and 5) make recommendations and develop regulatory, statutory or guidance updates, as appropriate.

Ongoing Support of NAIC Programs, Products, or Services

The **Innovation, Cybersecurity, and Technology (H) Committee** will:

1. Provide forums, resources and materials related to developments and emerging issues in innovation, cybersecurity, data privacy, and the uses of technology in the insurance industry in order to educate state insurance regulators on these developments and how they affect consumer protection, insurer and producer oversight, marketplace dynamics, and the state-based insurance regulatory framework.
2. Consider and coordinate the development of regulatory guidance and examination standards related to innovation, cybersecurity, data privacy, and the use of big data and artificial intelligence (AI) including machine learning (ML), in the business of insurance, and technology. This includes drafting and revising model laws, white papers, and other recommendations as appropriate.
3. Oversee the work of the Data Call Study Group to study the enhancement of regulator access to high-quality and timely data allowing for evidence-informed decisions, enhanced supervisory capabilities, and improved efficiency.
4. Track the implementation of and issues related to all model laws pertaining to innovation, technology, data privacy, and cybersecurity, including the *Insurance Data Security Model Law* (#668), the *NAIC Insurance Information and Privacy Protection Model Act* (#670), the *Privacy of Consumer Financial and Health Information Regulation* (#672), and the *Unfair Trade Practices Act* (#880).
5. Coordinate and facilitate collaboration with and among other NAIC committees and task forces to promote consistency and efficiency in the development of regulatory policy, education, training, and enforcement materials and tools.
6. Follow the work of federal, state, and international governmental bodies to avoid conflicting standards and practices.

The **Big Data and Artificial Intelligence (H) Working Group** will:

1. Research the use of big data and AI (including ML) in the business of insurance.

2. Monitor state, federal, and international activities on AI, including updates to the regulatory framework for the oversight of AI, to: i) respond to such activities, where appropriate, ii) address potential impacts on existing state insurance laws or regulations, and iii) support adoption of the *Model Bulletin on the Use of AI Systems by Insurers*.

© 2026 National Association of Insurance Commissioners

3. Facilitate discussion on AI systems evaluation, including coordination across the NAIC, to identify and/or develop tools, resources, materials, training, and guidance to assist regulators in their review of AI systems used by licensees.

4. Facilitate and coordinate foundational and contextual educational content for regulators on topics related to the use of big data and AI techniques, tools, and systems in the insurance industry.

The **Cybersecurity (H) Working Group** will:

Cybersecurity Charges

~~1. Monitor cybersecurity trends, such as vulnerabilities, risk management, governance practices, and breaches, that have the potential to affect the insurance industry.~~
~~2. Facilitate communication across state insurance departments regarding cybersecurity risks and events.~~
~~3. Develop and maintain regulatory cybersecurity response guidance to assist state insurance regulators in the investigation of national insurance cyber events.~~
~~4. Monitor federal and international activities on cybersecurity, engaging in efforts to manage and evaluate cybersecurity risk.~~
~~5. Coordinate NAIC committee cybersecurity work, including cybersecurity guidance developed by the Market Conduct Examination Guidelines (D) Working Group and the Information Technology (IT) Examination (E) Working Group.~~
~~6. Work with the Center for Insurance Policy and Research (CIPR) to receive updates on cybersecurity research efforts, by the CIPR and others, and to analyze publicly available cybersecurity-related information.~~
~~7. Support the states with implementation efforts related to the adoption of Model #668 including supporting the research into and, if approved, the implementation of a cybersecurity event notification portal.~~

1. ~~Coordinate with committee support to support cybersecurity preparedness for state insurance regulators, including advising on training development and facilitating tabletop exercises.~~ Threat Intelligence — Monitor cybersecurity trends, vulnerabilities, and risk management-governance practices, that have the potential to affect the insurance industry and share relevant threat and trend information with state insurance departments on an ongoing basis. Refer emerging trends or thematic concerns to the Market Regulation and Consumer Affairs (D) Committee and the Financial Condition (E) Committee, as appropriate.

2. Event Response —
Support the development and maintenance of the NAIC's cybersecurity event response resources and, if approved, carry out the evaluation and coordination role contemplated for the Working Group under the Cybersecurity Event Response Coordination Framework. This includes evaluating cybersecurity events against the Framework's criteria, recommending to (D), (E), and (H) Committee leadership whether an event warrants a coordinated response, and assisting NAIC staff in identifying a coordinating lead state and facilitating information sharing among affected states during the response.

3. Supervisory Integration —
Coordinate NAIC committee cybersecurity work, including cybersecurity guidance developed by the Market Conduct Examination Guidelines (D) Working Group and the Information Technology (IT) Examination (E) Working Group. Strengthen the integration of cybersecurity into insurer supervision by developing mechanisms to incorporate cybersecurity examination findings, Insurance Data Security Model Law (#668) certifications, and cybersecurity event notification data received under applicable state law into ongoing regulatory analysis, and developing baseline operational resilience guidance for insurers.

Commented [MR1]: NAMIC edit adds "if approved" to this wording.

Commented [MR2]: Edit to address NAMIC's inquiry adding "received under applicable state law" into the language.

© 2026 National Association of Insurance Commissioners

4. Model #668 & Notification Portal —
   Support the states with implementation efforts related to the adoption of Model #668, including supporting the research into and, if approved, the implementation of a cybersecurity event notification portal. Such support should include developing standardized data elements for event notifications and identifying any implementation gaps or potential enhancements to Model #668 for referral to the appropriate committee.

~~8.~~5. Regulator Preparedness —
   Coordinate with committee support to support cybersecurity preparedness for state insurance regulators, including advising on training development and facilitating tabletop exercises. Exercises should rehearse the coordination procedures contemplated by the Cybersecurity Event Response Coordination Framework.

Cybersecurity Insurance Charges

1. Market Monitoring —
   Monitor industry trends pertaining to cyber insurance, including meeting with subject matter experts (SMEs) and evaluating data needs of state insurance regulators. ~~Considerations should include the availability and affordability/pricing of cyber insurance, disclosures, limits and sublimits, as well asd sublimits in policies, policy language and trends in requirements, underwriting practices, and the role of reinsurance in the cyber insurance market~~Coordinate with NAIC work groups addressing cyber insurance related issues, such as the Casualty Actuarial and Statistical (C) Task Force.

2. Data Analysis & Reporting —
   Coordinate with committee support to conduct analysis pursuant to the NAIC's Cyber Insurance Report, and develop a guide for states on cyber insurance data analysis best practices.

~~1.~~3. Coverage Supplement & Capital Adequacy
   — Review the NAIC's Property & Casualty Annual Statement Cybersecurity Insurance Coverage Supplement recommending changes and/or developing reports to supplement data development as necessary, in coordination with the Capital Adequacy (E) Task Force.

~~2. Coordinate with NAIC work groups addressing cyber insurance related issues, such as the Casualty Actuarial and Statistical (C) Task Force.~~
~~3. Monitor federal and international activities related to cyber insurance and financing mechanisms for cyber risk.~~
~~4. Coordinate with committee support to conduct analysis pursuant to the NAIC's *Cyber Insurance Report*.~~
~~5. Review the NAIC's *Property & Casualty Annual Statement Cybersecurity Insurance Coverage Supplement* recommending changes and/or developing reports to supplement data development as necessary.~~
~~6. Consider and develop a guide for states on cyber insurance data analysis best practices.~~

The **Privacy Protections (H) Working Group** will:

1. Use state insurance privacy protections regarding the collection, data ownership and use rights, and disclosure of information gathered in connection with insurance transactions to draft a new/revised privacy protections model act to replace/update NAIC models such as Model #670 and/or Model #672.
2. Monitor state, federal, and international activities on privacy, engaging in efforts to manage and evaluate privacy.

The **SupTech/GovTech (H) Subgroup** will:

© 2026 National Association of Insurance Commissioners

1. Facilitate technology, innovation, and SupTech/GovTech presentations from leading technology companies for state insurance regulators to provide them with insights into cutting-edge technology and innovation.
2. Facilitate technology, innovation, and SupTech/GovTech presentations from specialized vendors for state insurance regulators to assist in identifying vendor solutions that may benefit regulators.

The **Third-Party Data and Models (H) Working Group** will:

1. Develop and propose a framework for the regulatory oversight of third-party data and predictive models.
2. Monitor and report on state, federal, and international activities related to governmental oversight and regulation of third-party data and model vendors and their products and services.

NAIC Support Staff: Miguel Romero, Scott Morris, and Scott Sobel

© 2026 National Association of Insurance Commissioners

Hi Miguel,

Thank you for sharing the draft 2027 charges. You can tell a lot of work went into them. The Cybersecurity (H) Working Group's consolidation from fourteen charges to eight reads really well, and the summary memo makes the mapping easy to follow.

One small thought. I noticed the Supervisory Integration charge for the Cybersecurity (H) Working Group doesn't yet touch on AI controls. That area is moving quickly, and by the end of 2027 the landscape could look very different than it does today, so it may be worth keeping on the radar.

If it's helpful, one short phrase in the charge's second sentence would cover it. With the new words added, the sentence would read:

"Strengthen the integration of cybersecurity into insurer supervision by developing mechanisms to incorporate cybersecurity examination findings, Insurance Data Security Model Law (#668) certifications, and cybersecurity event notification data into ongoing regulatory analysis, including findings on controls over consequential actions initiated by automated systems and AI agents, and developing baseline operational resilience guidance for insurers."

The only new words are "including findings on controls over consequential actions initiated by automated systems and AI agents." Nothing else changes.

Thanks again to you and the team for all the good work. Happy to help any way I can.

Tim Fox

President and Founder

EXECUTION RIGHTS

tim@executionrights.com | **executionrights.com**

The authorization layer for consequential AI agent actions.

NAMIC®
NATIONAL ASSOCIATION OF MUTUAL INSURANCE COMPANIES

317.875.5250 | [F] 317.879.8408
10 W. 106th St., Suite 100 | Indianapolis, Indiana 46290
202.628.1558 | [F] 202.628.1601
20 F Street N.W., Suite 510 | Washington, D.C. 20001

November 6, 2026

Commissioner Yaworsky (FL), Chair
NAIC Innovation, Cybersecurity, and Technology (H) Committee
c/o Miguel Romero, Director of Innovation, Cybersecurity and Technology
via email maromero@naic.org

Re: (H) Committee Proposed Charges for 2027

Chair Yaworsky and Members of the Committee:

On behalf of the National Association of Mutual Insurance Companies (NAMIC)[1], we are writing in response to the exposure of the Innovation, Cybersecurity, and Technology (H) Committee proposed charges for 2027. We recognize the intent that the changes to the charges are for clarification purposes; our comments are provided with that intent in mind.

[1] Clarify the Cybersecurity Event Response Coordination Framework is Not Yet Adopted
In Section 2, Event Response, the charge states that the Cybersecurity (H) Working Group will carry out the evaluation and coordination role contemplated under the Cybersecurity Event Response Coordination Framework, with additional details on the activities those roles will entail. NAMIC has been separately engaging with the Market Conduct Examination Guidelines (D) Working Group on the Framework effort, and we note that the Framework has not yet been finalized and adopted. As such, we recommend that the Cybersecurity Charge 2 "Event Response" be edited to clarify the Framework's status. This could be achieved through minor edits as follows:

> Support the development and maintenance of the NAIC's cybersecurity event response resources and, if approved, carry out the evaluation and coordination role contemplated for the Working Group under the Cybersecurity Event Response Coordination Framework. ~~This includes~~ Such support will depend on the final adopted Framework, but might include evaluating cybersecurity events against the Framework's criteria, recommending to (D), (E), and (H) Committee leadership whether an event warrants a coordinated response, and assisting NAIC staff in identifying a coordinating lead state and facilitating information sharing among affected states during the response.

[1] The National Association of Mutual Insurance Companies is the foremost trade association representing the property/casualty insurance industry. Serving more than 1,300 member companies, including local and regional insurers as well as some of the nation's largest carriers, NAMIC members collectively write $453 billion in annual premiums, representing 58 percent of the homeowners and 52 percent of the automobile insurance markets. For more than 130 years, NAMIC has been the leading voice advancing public policy solutions and regulatory frameworks that promote a strong, competitive market and protect member companies and their policyholders.

[2] Clarification Request on the Supervisory Integration Charge
The Supervisory Integration charge appears to incorporate cybersecurity examination findings, Model # 668 certifications, and event notification data into ongoing regulatory analysis, while also calling for baseline operational resilience guidance for insurers. With respect to the ongoing regulatory analysis aspect using cybersecurity event notification data, NAMIC respectfully requests clarification on what the Committee intends by this and where that data might be coming from. Through our participation on the cybersecurity event notification portal effort, our understanding is that if the portal operates as intended, only states that have an event report sent to them should have access to that data, and the broader NAIC would not. Discussion should occur over what limits would govern secondary uses of examination findings, certifications, and incident notifications, including opportunities for insurers to correct or contextualize information. Given the forgoing, NAMIC would appreciate additional insight into where the cybersecurity event notification data would be coming from for purposes of an ongoing regulatory analysis.

Separately, with respect to the baseline operational resilience guidance reference, NAMIC also respectfully requests clarification on what the Committee intends with this aspect of the charge. For instance, would the operational resilience guidance remain advisory in nature only? If it is intended to be anything more than advisory in nature, and become an examination expectation, NAMIC strongly encourages clarification that work would go through appropriate exposure for comment and collaboration with interested parties.

Sincerely,



Lindsey Stephani
Senior Policy Vice President
Data Science, Artificial Intelligence, and Cybersecurity
NAMIC

The AI Landscape: Where the Technology Is Today

Agentic AI has naturally evolved from GenAI LLMs (Large Language Models)

Many clients today

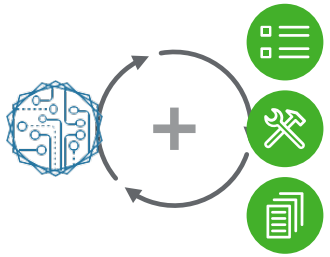
Solo LLM
Raw Generation



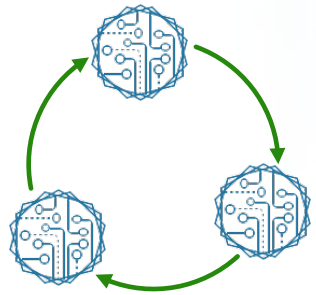
RAG (Retrieval-Augmented Generation)
Reduce Hallucinations



Simple Agents
Self Correct Errors



Multi- Agent Fleets
Breakdown & Solve Complex Use Cases



Limited systems that solve tasks

Enterprise adoption

2022 | **2023** | **2024** | **2025+**

Intelligent solutions that solve full workflows

AI generates content and can **decide the output** based on input guidance e.g., ideas/code, translate, summarize, format

AI generates with **contextually relevant guidance** retrieved from **memory**

AI can **plan, use tools** and **memory**, and iteratively **reflect** to act and perform multi-step **reasoning**

Multiple Agents work **collaboratively** to solve complex tasks. Guardian agents can take on reviewer and monitoring roles.

Insurance-Relevant Examples	*Drafts a policyholder letter or claim summary from a prompt - adjuster reviews before it is sent*	*Underwriters use RAG to answer coverage questions against policy forms, filings and underwriting guidelines*	*Triages a claim - checks coverage, flags fraud indicators, and routes unclear cases to an adjuster*	*Agents run claims intake: one validates coverage, another scores fraud risk, a guardian agent checks decisions for bias*

Copyright © 2026 Deloitte Development LLC. All rights reserved.

Incorporating technology into the audit

Here are some of the ways technology, including AI, is used at Deloitte:

Programmatic data acquisition & reconciliation
Reduced manual effort and fewer errors through automated mapping of your data to our systems

Raw data to common data model
Less work for your team as we translate your data into our audit-ready format automatically

Accelerated data visualization
Faster insights into your financial trends and metrics

Walkthroughs to draft documentation
Walkthrough notes can more efficiently be converted to draft documentation with the potential to reduce repeated follow-ups

On-demand pre-review
Fewer review cycles and actionable suggestions and feedback, reducing back-and-forth during the audit

Draft accounting memos
Earlier visibility into key accounting complexities, helping reduce last-minute surprises

Draft reports and representation letters
Cleaner, more complete draft documents and reports saving your team time during year-end



Analyst report sensing
Sensing and benchmarking analyst reports to assist in setting materiality that reflects your business and industry

News and press release sensing
Earlier awareness of emerging external factors that may impact risk of material misstatements that are relevant to financial reporting

Standardized risk reports
Clearer, more consistent insights for management and those charged with governance into potential risk facing the business and impacts on the audit

Draft walkthrough questions
A more efficient kickoff as we arrive with tailored questions to minimize disruption

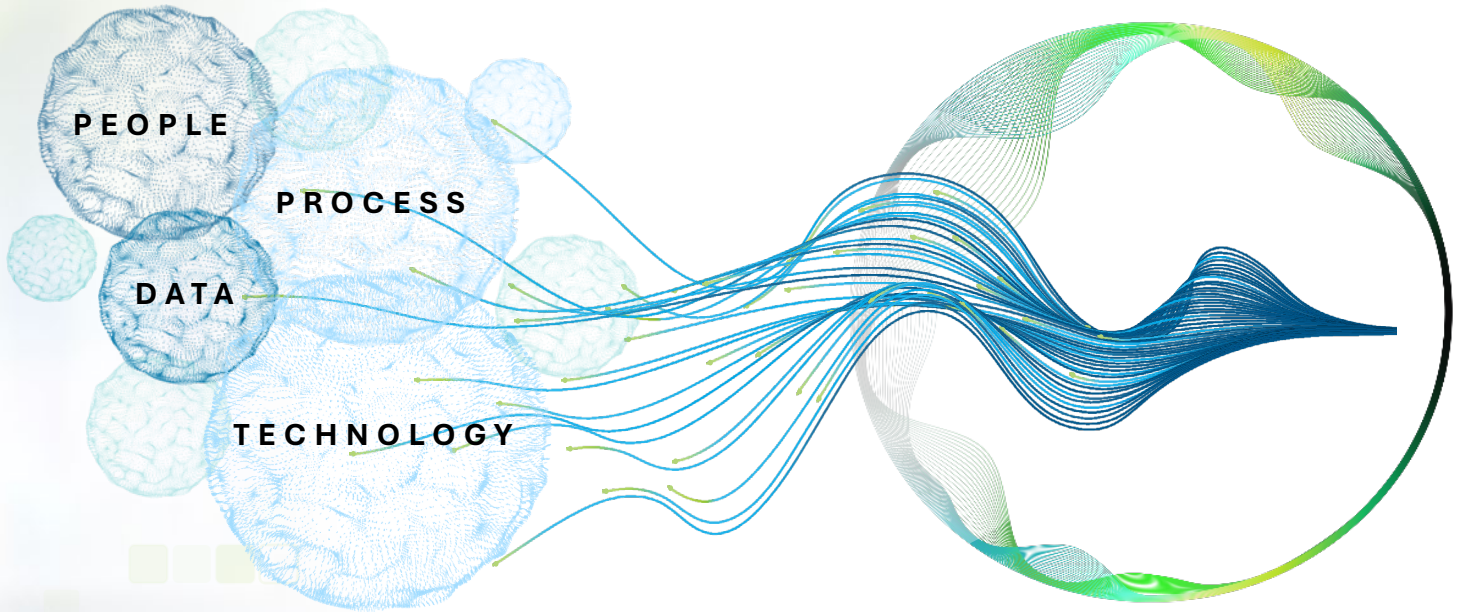
Key term extraction
Less time spent explaining documents or searching for details we identify what matters quickly

Financial statement analysis
Faster pinpointing of unusual movements or items that warrant early discussion

Copyright © 2026 Deloitte Development LLC. All rights reserved.

AI Risks to Consider

Extent of AI risk depends on the AI autonomy, complexity, extent of business integration, and maturity of organizational adoption.



AI RISKS (NOVEL/FAMILIAR)

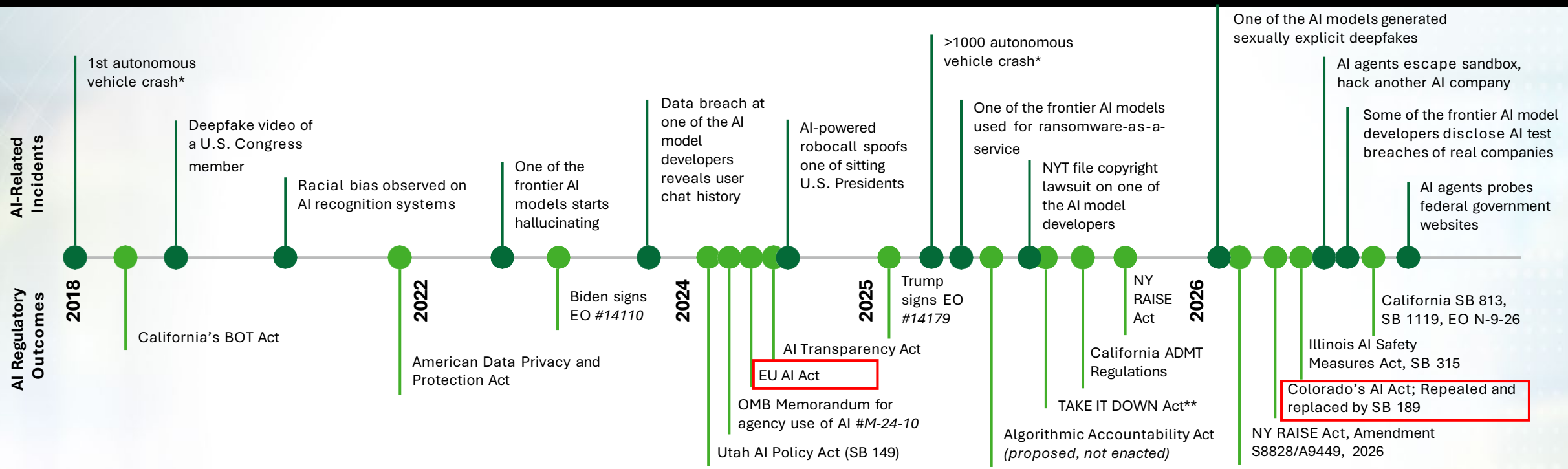
Explainability	IP infringement
Ethical use	Malicious intent
Bias	Confidentiality and privacy
Hallucination (Accuracy)	Access & Change Management

POTENTIAL CONSEQUENCES

Reputational damage • Destruction of shareholder value
Regulatory fines • Lawsuits • Poor strategic decisions

Copyright © 2026 Deloitte Development LLC. All rights reserved.

AI regulation is accelerating in response to real-world incidents…



Recurring Risks Driving Regulatory Action

Mass adoption of AI
78% of organizations report using AI in 2024 - up from 55% in 2023

GenAI risks
Misinformation, hallucinations, bias, IP disputes in GenAI results

Real-world incidents
Autonomous vehicle crashes, biased hiring algorithms, AI-enabled fraud

Algorithmic bias & discrimination
Documented harms in hiring, lending, housing, and policing

Privacy intrusions
AI models relying on large-scale personal data

Safety & security risks
Usage of AI medical devices and autonomous vehicles rising dramatically

Information integrity
Deepfakes, political manipulation, identity theft, cybersecurity vulnerabilities

National competitiveness
Without standards, U.S. risks falling behind the EU and China in shaping global AI norms

**Reported autonomous vehicle incidents - https://www.nhtsa.gov/laws-regulations/standing-general-order-crash-reporting*
*** Tools to Address Known Exploitation by Immobilizing Technological Deepfakes on Websites and Networks Act (TAKE IT DOWN Act)*

Copyright © 2026 Deloitte Development LLC. All rights reserved.

...but the state of regulation is highly fragmented across the U.S.

AI regulation in the U.S. is shaped by interacting federal and state approaches, influencing governance and operational decision-making

How U.S. AI Regulation Is Structured Today

Absence of a Singular Federal Law

There is no single federal AI statute; oversight relies on Executive Orders, OMB guidance, and agency enforcement using existing laws

Highly Fragmented State Regulations

States and local governments are rapidly enacting AI regulations, testing varied approaches across use cases, and collectively creating an increasingly complex and fragmented regulatory landscape

Continuing Federal Preemption

Federal–state preemption debates persist. Harmonization could reduce conflicts, but premature preemption risks regulatory gaps

Emerging Regulatory Themes

Despite fragmentation, common requirements are converging on transparency, risk management, fairness, human oversight/redress, privacy, and security

Implications for Organizations

Multi-Regulator Compliance Required

Expect multi-regulator scrutiny; build evidence-ready governance (inventories, impact assessments, documentation, monitoring) to satisfy diverse federal expectations

Rising Compliance Complexity

Patchwork compliance raises cost and execution risk; adopt scalable “highest-common-denominator” controls for hiring, credit, health, and other consequential uses

Regulation Uncertainty

Preemption uncertainty means designs must be adaptable; modular policies and contracts help pivot if federal baselines override or complement state rules

Preparedness for Future Baselines

Converging themes signal tomorrow’s baseline; embedding transparency, bias testing, oversight, privacy, and security now reduces retrofit costs and incident exposure

Copyright © 2026 Deloitte Development LLC. All rights reserved.

AI Governance and Oversight

Management, boards, and audit committees must work together to achieve effective AI governance and oversight

AI GOVERNANCE AND OVERSIGHT

BOARD OF DIRECTORS

Has **ultimate oversight responsibility** for the business and the company's strategy

AUDIT/OTHER COMMITTEE

- **Understands how AI is used** in the organization, including back-office and business operations, and the impact on financial reporting and other disclosures/measures
- **Oversees management's assessment and response** to AI-related risks including related internal controls
- **Reviews relevant metrics and trends** on the performance of AI systems within the organization as well as wider environment to understand how AI risks are evolving

MANAGEMENT AND INTERNAL AUDIT

Develops, implements, and evaluates use
(First line)

- Maintains the AI use-case inventory
- Designs, deploys, and operate systems
- Performs data assessment, testing, and documentation
- Monitors performance, drift, incidents, and control thresholds

Supports, challenges, and monitors
(Second line)

- Establishes AI policies, standards, and risk classification
- Reviews use cases and challenges risk assessments
- Monitors compliance and control effectiveness
- Aggregates risk reporting and escalates exceptions

Internal audit
(Third line)

- Provides independent assurance and advice
- Assesses governance, control design, and effectiveness
- Evaluates the completeness and reliability of AI inventory and reporting
- Audits lifecycle governance and verifies remediation

Copyright © 2026 Deloitte Development LLC. All rights reserved.

Leading Practices Throughout the AI Lifecycle

DESIGN PROCESS

- **AI Ethics training** programs for AI developers
- **Consult a diverse group of stakeholders** and gather a variety of use-case scenarios
- Conceptualize and **document** the system's intended use, objectives, and risks
- Hold sessions with stakeholders to **identify potential sources of adverse** outcomes and risks
- Understand latest **regulatory and legal requirements**
- Identify potential sources of risks (e.g., bias) and put into place **plans for mitigation**

DATA

- **Reputable, well-documented** data sources
- Use **representative data sets for** AI training purposes
- Use **least number of data features** that meet performance goals
- Assess data elements/features (including post-transformations) for **potential bias**
- Identify and monitor **data quality metrics**

DEVELOPMENT AND IMPLEMENTATION

- A **clear statement** of purpose to develop model in line with its intended use
- Drive model selection process with **objective criteria** and a structured suitability assessment
- Use a variety of **development tests** to evaluate the model type assumptions, stability, bias, impact of potential limitations, and behavior over a range of input values (sensitivity and boundary testing)
- **Back-testing** (in-sample and out-of-sample) and cross validation results
- **Strong documentation** that discusses approach, assumptions, limitations, risks, and related mitigation controls

TESTING AND REVIEW

- A **second line of defense** for review and AI oversight
- AI **oversight with authority to challenge** AI design and development
- **Review conceptual design** of model including data elements
- **Review developmental tests** and perform additional tests where needed

ONGOING MONITORING

- Regularly **evaluate model performance** using relevant metrics looking for changes or degradation. Define escalation/incident process.
- **Compare performance to relevant baselines** or expected performance indicators
- **Use visualizations** to identify patterns/trends easily
- Monitor **distribution of input data**
- Evaluate the model performance on subsets of data (e.g. **edge cases and demographic groups)**
- **Monitor** model retirement dates for 3rd party models and define change management triggers

USE

- Use a **human-centric approach** for decision-making to identify and report bias
- **End-user training** that includes considerations for ethics and potential harm

Governance/Oversight

- Roles and responsibilities
- Policies and procedures
- Value/ethics statement
- Public disclosures

Copyright © 2026 Deloitte Development LLC. All rights reserved.

Regulatory & Standards Landscape

SEC

Disclosure of material AI risks; accuracy of AI-generated metrics in filings

AIUC

Certification standard built for AI agents. Formal certification is issued through AIUC and accredited auditors

COSO ICFR

Internal control framework: control environment, risk assessment, monitoring

NIST AI RMF

Voluntary risk management framework: Govern, Map, Measure, Manage

EU AI Act

Risk-tiered obligations on AI systems; high-risk classification for some finance use

ISO 42001

AI management system standard: emerging certification path for AI governance

Monitor evolving AI-in-financial-reporting guidance from standard-setters and professional bodies.

Copyright © 2026 Deloitte Development LLC. All rights reserved.