Building an AI Compliance Framework

David T. Vanalek and Kaitlin Hutson

I. Introduction

As has been the case historically, the rate at which technology evolves is much faster than legislation and regulations can keep up with. While there do not appear to be any federal statutory schemes in place currently regarding the use of artificial intelligence ("AI") tools and systems, the country has begun to see industry-specific guidelines, as well as recent statewide regulation. Despite the current lack of widespread regulation, there are serious ethical, privacy and data security considerations that must be addressed as the world enters a new technological era, and many regulatory bodies have promulgated guidance to mitigate against the risks associated with AI usage, including bias reinforcement, AI hallucinations, and other data security challenges. With advancements in AI systems comes various benefits in efficiency and accuracy for the ultimate benefit of the customer, so it is important to stay mindful and educated on how AI systems work and are used.

II. NAIC Model Bulletin

The National Association of Insurance Commissioners (NAIC) released a Model Bulletin, *Use of Artificial Intelligence Systems by Insurers*, in December 2023. The bulletin outlines guidelines which insurance companies are expected follow to comply with legal and regulatory standards surrounding fair trade practice, and is a good bellwether for other industries. Insurers are expected to "develop, implement, and maintain a written program (an 'AIS Program') for the responsible use of AI systems that make, or support decisions related to regulated insurance practice." Following a principles-based approach, the NAIC guidelines for AI governance focus on the following key requirements for AI systems: (1) fair and ethical; (2) compliance with existing laws; (3) accountability; (4) transparency; and (5) safe, secure, and robust systems. Any AI regulation framework appears to follow the same general approach. The Model Bulletin provides a great framework not only for insurers, but universally for businesses across all markets.

The processes for each business's AIS Program will depend on individual assessment of the degree and nature of the risks being posed to consumers by the use of AI systems, but the main considerations are: (1) nature of the decisions being made, informed, or supported by the AI system; (2) type and degree of potential harm; (3) the extent to which humans are involved in the final decision; (4) transparency an explainability to consumers; and (5) the extent and scope of the insurer's reliance on third-party data, predictive models, and AI systems.

General AIS Program guidelines are meant to help mitigate the risk of adverse consumer outcomes from usage of AI systems, addressing (1) corporate governance, (2) risk management controls, and (3) internal audit functions.

1. Insurers and businesses alike should address oversight of AI systems being used, including policies, processes, and procedures to be followed from development to retirement of an AI system; an accountability structure, such as the formation of an AI committee; development and implementation of ongoing training; and chains of command. This is important, especially with predictive models, for preventing performance issues and discrimination.
2. Risk management and internal controls policies should make sure to balance the benefits of automated AI systems with the risks associated. This includes addressing data practices, inventories of predictive models, documentation of development of systems, and testing/retesting models.
3. If the company is acquiring, using, or relying on third party data or AI systems, establishment of proper auditing procedures is necessary to ensure that legal standards are being met. Special attention must be paid to terms in third party contracts which provide audit rights to the business as a method of assessing third party data and/or AI systems, as well as cooperation with regulatory inquiries and investigations of the business.

At the time of this writing, the Model Bulletin has been quickly adopted with little or no changes by eleven states so far, including Alaska, Connecticut, Illinois, Kentucky, Maryland, Nevada, New Hampshire, Pennsylvania, Rhode Island, Vermont, Washington. Washington, DC has also adopted the Model Bulletin. Many more states are anticipated to follow with similar standards, or perhaps more restrictive standards, across the country. In addition, Colorado has recently become the first state to pass a comprehensive AI regulation law, applying not only to insurance companies, but various industries and companies doing business in the state.

III. State Law – Colorado

On May 17, 2024, Colorado's governor signed the Artificial Intelligence Act (Senate Bill 24-205), which applies to all "developers" and "deployers" of "high-risk artificial intelligence systems." These high-risk AI systems are defined as AI systems which make or are a substantial factor in making "consequential" decisions. Examples of consequential decisions include employment or education opportunities, financial services, essential government services, healthcare services, housing, insurance, and legal services. AI systems that are not intended to replace human review, such as those which perform only small tasks, are not included in this regulation.

A "developer" is defined as a person who develops or substantially modifies an AI system, and a "deployer" is a person who uses high-risk AI Systems. Developers and deployers are both obligated to use reasonable care to avoid algorithmic discrimination. For developers, this means making specific information about the AI system transparent and available to deployers, making a public statement on any known or foreseeable risks, and disclosure to the state attorney general on any foreseeable risk of algorithmic discrimination within 90 days of discovery. For deployers, this means implementing a risk management policy, conducting impact assessments, notifying consumers of how the high-risk systems are making decisions about them, and disclosing discovery of algorithmic discrimination to the attorney general within 90 days. Enforcement of this law is exclusive to the state attorney general's office, which has discretion to implement further rules.

This law loosely mirrors the NAIC AI Model Bulletin in many ways, but this extends to encompass many different types of businesses and industries who may be starting to use new and emerging AI systems. Both the Model Bulletin and the Colorado AI law include implementation of a risk management policy or program, assessments/audits to prevent discrimination, and transparency of consumer rights and impacts. While this law does not go into effect until February 1, 2026, it is the first AI compliance framework from a state statutory perspective. As federal interest in AI regulation and legislation is starting to take shape, there is a good chance that many states will be implementing versions of their own AI compliance frameworks.

IV. Federal Interest

Apart from various proposals from the US Senate and House, as well as AI guidance from the White House, the United States Department of the Treasury recently stated in its *Request for Information on Uses, Opportunities, and Risks for Artificial Intelligence in the Financial Services Sector*, the Treasury is seeking comment on the uses of AI in the financial services sector and the types of opportunities and risks associated with usage of AI systems. This request for information ("RFI"), published on June 6, 2024, presents a 60-day period for the Treasury to gather public comment. Input is not only being sought from financial institutions, but any "impacted entities," including consumers, investors, financial institutions, businesses, regulators, etc.

The Treasury has been exploring this subject since November 2023, in terms of how AI is impacting different financial related markets. As new and emerging technology is being developed, the Treasury is seeking more information on these systems, as new challenges come along with them. The Treasury leans on explainability of AI systems and how they make decisions, as there is concern about what level of understanding financial institutions have on what data is being used to train the AI systems and how bias can occur. Consumer protection and data privacy are other key issues being addressed in the RFI, and how AI models require great amounts of data for training and operating. It is important to make sure that consumer data is being properly protected.

The Treasury specifically mentions the NAIC AI Model Bulletin, pointing out that this document provides guidance and asking what changes insurers have implemented to comply and be consistent with the regulatory guidance. The Treasury mentions that states are beginning to develop their own regulations and wishes to gain information on how these regulations and laws are being followed. This RFI shows that there is increasing interest surrounding AI usage and compliance, now at a federal level. While there is no current federal legislation regarding the use of AI systems, all industries should continue to monitor any developments at the federal level.

V. Conclusion

Companies should establish an AI compliance framework that fits their business and specific utilization of AI systems, as business needs will vary across different industries. The NAIC AI Model Bulletin gives a solid framework for businesses to use as a starting point, and the Colorado AI law provides an example of the types of AI regulatory laws that we might look forward to going forward, as other states will likely implement their own versions of AI regulations and compliance as AI is utilized more and more in everyday business to serve its customers.