

Legal & Risk Considerations for Local Government Use of AI

Presented by:

Sam Light, CIRSA Deputy Executive Director/General Counsel Nick Cotton-Baez, CIRSA Associate General Counsel April 24, 2025



Introduction

- The rapid advancement of artificial intelligence (AI) has transformed various sectors of the economy, and local government is no exception.
- AI has the potential to transform the way local governments operate and serve their constituents.
- As local governments navigate the implementation and use of AI in government operations, it's crucial for local government officials to understand both the opportunities and risks.
- This presentation addresses key questions for local governments desiring to harness the power of AI tools in local government, with an emphasis on managing legal and liability risks.



Presentation Overview

Topics:

- I. Demystifying Al
- II. Legal and liability risks AI tools
- III. Suggestions for safe and efficient use of AI tools
 - A. Readiness
 - B. Selection
 - C. Contracting



I. Demystifying Artificial Intelligence

- Artificial intelligence is hard to define because AI tools are capable of a wide range of tasks and outputs.
- Senate Bill 24-205: "Artificial intelligence system" means any machine-based system that, for any explicit or implicit objective, infers from the inputs the system receives how to generate outputs, including content, decisions, predictions, or recommendations, that can influence physical or virtual environments. (Not the most helpful!)
- Basically, AI is a broad field aimed at creating intelligent machines capable of performing tasks typically requiring human intelligence, such as learning, reasoning, problem-solving, perception, and decision-making.
- We encourage you to think about AI as a tool in service of your organization's work. As with any other tool, you are responsible for its outcomes!



Applications In Local Government

- Drafting: Policies, memos, financial narratives
- **Chatbots:** Utilize organization-specific information to provide basic responses to customers (e.g., bill payment) and employees (e.g., HR payroll/benefits)
- **Transcription:** Real-time audio transcription (accessibility); meeting minutes, hearing transcripts
- **Traffic management:** Predictive road maintenance, optimizing signal timings, optimizing bus routes, enforcing parking and speed limits
- Water system management: Predicting pipe failures, smart irrigation systems, automated inventory of service lines and materials
- "Digital twins": Virtual model used to predict the outcomes of different changes within a complex infrastructure system
- **Billing:** Auto-generation of invoices and past-due utility bills

- Short-term rental monitoring: AI "crawlers" can identify advertisements for short-term rentals not properly licensed
- **Cybersecurity:** Cyber-risk management/analysis, auto-generated phishing emails (training)
- **Disaster management:** Predict weather events/risks using satellite imagery, physical sensors, historical data; enable efficient emergency response
- Fraud/scam detection: Identifying fraud in unemployment claims; taxes
- **HR/Employment:** Hiring, workflow & benefits tools
- Law enforcement: Enhancing efficiency and precision in crime prevention and investigation
- **Legal:** Legal review, document automation, predictive analysis, and client communications
- Other?



Two Broad Functions

- •AI tools commonly used in local government generally incorporate one or both of the following functions:
 - Identifying patterns in controlled data sets to classify data for distinct treatment.
 - Generating content (outputs) based on prompts (inputs) and inferences drawn from a dataset on which the program has been trained.



Generative Al

- "Generative AI" is a subset of AI that refers to systems utilizing algorithms and statistical models to process, categorize, analyze, and draw inferences from patterns in the dataset on which the program has been trained—e.g., large language models ("LLMs")—to generate statistically probable outputs, such as text, images, and videos, when prompted by users.
- Popular Generative AI tools and platforms include Open AI's ChatGPT, Microsoft's Copilot, and Google's Gemini, among many others.
- How does it work?
 - □ User prompts by asking a question or making a request.
 - Works similarly to the "autocomplete" function when typing in a search bar or texting, by finding patterns in text and predicting what word should come next within the context of the prompt—repeats the process.
 - However, "machine learning" and the scale of data underlying the algorithm (LLM) makes its predictions much more sophisticated.
 - "Machine learning" algorithms allow AI tools to train themselves on large amounts of data to "learn" trends and make informed predictions—continuous "retraining" as new data/feedback is introduced.



II. Legal And Liability Risks – AI Tools

- By now, you've likely come across ominous warnings about AI's potential to surpass human intelligence, giving AI systems the ability to undertake actions beyond human control, potentially in malicious ways that may pose existential threats.
- Maybe you fear (or are addressing fears of) Al's potential to increase government surveillance and social manipulation, leading to the erosion of citizen privacy and enabling authoritarian control.
- While these and other potential outcomes shouldn't be ignored, whether they become existential threats is largely out of local governments' control.
- More practically, there are known AI risks that local governments can control and minimize by implementing sound policies and training programs for the appropriate and responsible use of AI in local government services and functions.



AI Legislation?

- Until recently, state and federal laws addressing AI mostly focused on AI developers (e.g., OpenAI, Google, Microsoft).
- However, recent Colorado legislation, which takes effect February 1, 2026, extends to local governments that develop or use AI systems to make—or use it as a substantial factor in making—"consequential decisions" (e.g., decisions involving the provision or denial of employment or essential government services).
- In any case, don't wait for comprehensive state or federal regulation...take steps to protect your organization now!



Other Laws?

- While AI regulation is still in its early stages, AI tools implicate a variety
 of laws addressing data privacy, confidentiality, technology accessibility,
 and copyright/intellectual property.
 - Data Privacy/Security: C.R.S. § 24-73-101, *et seq.* (protecting personal information and PII).
 - □ Open records: C.R.S. § 24-72-201, *et seq.* (CORA) (prohibiting disclosure of certain confidential and sensitive information).
 - Technology Accessibility: C.R.S. §§ 24-85-101 through -104 and 24-34-802 (requiring public entity compliance with statewide accessibility standards).
 - Intellectual property: Title 35, United States Code (protecting patents, copyrights, trademarks, and trade secrets).
- Remember: AI is a tool and your organization is responsible for outcomes involving AI tools. Therefore, AI really implicates ALL laws governing local governments and their officials!



Generative AI Risks - User Prompts

- User prompts and AI-generated responses generally are not private, as Generative AI models recycle and learn from previous interactions (i.e., prompts and responses) with users.
- If used in prompts, security breaches involving Generative AI systems may contain personal information or personally identifying information and other sensitive and confidential information, which could give rise to violations of data privacy, open records, or other laws.
 - *e.g.,* C.R.S. § 24-73-101, *et seq.* (requiring a government entities to implement and maintain reasonable security procedures for the protection of PII).
 - *e.g.,* C.R.S. § 24-72-204 (CORA) (prohibiting disclosure of names, addresses, telephone numbers, and personal financial information of past or present users of public utilities, public facilities, or recreational or cultural services).
- Use of Generative AI may result in the creation of a public record subject to disclosure under the Colorado Open Records Act (CORA).



Generative AI Risks – Content

Generative AI systems are most-often trained on data sourced from the internet, which may produce **inaccurate or fictitious** responses to prompts, content reflecting the **biases** of such data, or content containing **copyrighted material**.

- **Inaccuracy:** Generative AI systems are only as accurate as the source materials on which they're trained!
- Hallucinations: Generative AI is designed to make up information when it does not have an answer, which
 may lead to inaccurate responses because the data it's using is incomplete or inaccurate. In some cases,
 Generative AI has even been observed to "hallucinate" website URLs, court cases, and other purported source
 materials.
- **Bias:** Generative AI systems can reflect the biases (e.g., cultural, political, social, etc.) of the source materials on which the system has been trained because they cannot compensate for preexisting prejudices, stereotypes, or underrepresented data sets.
- **Copyright/IP Infringement:** Generative AI systems are trained using data that has been sourced from the internet, often without regard to copyright or licensing terms, and it's often difficult to determine the content used to train a Generative AI system, and the extent to which AI-generated content regurgitates copyrighted material.
 - Basis for many lawsuits brought against Generative AI developers by artists, authors, and other content creators.
 - □ Potentially heightened risk in AI-generated images and videos.



ChatGPT "Hallucination"

We asked ChatGPT about the "willful and wanton" exclusion from a public entity's obligation under the CGIA to indemnify employees for claims arising from acts or omissions occurring during the performance of job duties and within scope of employment...

is there a case that extends the exclusion to criminal acts?

Yes, there is a significant case that helps clarify the exclusion of indemnification for criminal acts under the Colorado Governmental Immunity Act (CGIA): **Berkeley v. Denver** (2012). This case illustrates the principle that public entities cannot indemnify employees for liability arising from criminal acts.

In Berkeley v. Denver, the plaintiff, a former police officer, sought indemnification for damages after he was found liable for violating civil rights under 42 U.S.C. § 1983. His actions, which included using excessive force, were determined to be willful and wanton, a standard that overlaps significantly with criminal conduct. Although the case involved civil rights violations, the ruling emphasized that willful and wanton conduct (which frequently involves criminal behavior) is outside the scope of indemnification by the public entity under the CGIA.

ChatGPT "Hallucination" (Cont.)

what is the citation for Berkeley v. Denver

The correct citation for Berkeley v. Denver is:

Berkeley v. Denver, 262 P.3d 1119 (Colo. App. 2011).

This case was decided by the Colorado Court of Appeals in 2011, and it provides insight into the application of the Colorado Governmental Immunity Act, particularly regarding indemnification exclusions for willful and wanton conduct.

this case does not exist

Apologies for the confusion earlier. You are correct that **Berkeley v. Denver** does not exist. I appreciate your patience.

Hallucination & Real Life Risk?

- Colorado attorney used ChatGPT to generate case citations and case-specific details to support his motion to set aside an unfavorable district court decision entered against his client. The lawyer filed the motion without verifying whether the cases existed, and when the judge noticed the cited cases did not exist, the lawyer lied about his use of ChatGPT, blaming the fictitious citations on an intern. The events led to suspension of the attorney's law license.
- "NYC's AI chatbot was caught telling businesses to break the law. The city isn't taking it down." <u>https://apnews.com/article/new-york-city-chat</u> <u>bot-misinformation-6ebc71db5b770b9969c906</u> <u>a7ee4fae21</u>

Is Hallucination Harm on Your Entity's / Your Staff's Risk Radar?



Bias – Case Study

- AI facial recognition used in law enforcement software has been found to misidentify black faces at a higher rate than white faces and exhibited racial profiling biases.
- In Detroit (2020), Robert Williams was the first innocent person known to be wrongfully arrested based on faulty AI facial recognition.
- Several other wrongful arrests followed, subjecting the City of Detroit to lawsuits and intense scrutiny from the ACLU.
- See this NYT article:

https://www.nytimes.com/2024/06/29/technology/detroit-facial-recognition-falsearrests.html; see also, this AACP policy brief, The Use of Artificial Intelligence in Predictive Policing: https://naacp.org/resources/artificial-intelligence-predictive-policing-issue-brief.



Risks In Employment?

- The use of AI to inform employment decisions (e.g., hiring selection, pay determinations, and performance monitoring) may run the risk of violating Title VII of the federal Civil Rights Act of 1964, the Age Discrimination in Employment Act (ADEA), the ADA, or other employment laws.
- The EEOC had published technical guidance on how to measure adverse impact when employment selection tools use AI, and uniform guidelines concerning use of AI in employee selection procedures. However, the guidance has since been scrubbed from the EEOC's website.
- Still, local governments should expect to be held responsible for adverse impacts arising from the use of AI in employment decisions! See Mobley v. Workday, Inc., 740 F.Supp.3d 796 (N.D. Cal. 2024) (federal anti-discrimination statutes do not distinguish between delegating functions to an automated agent versus a live human one).
- As noted above, effective February 1, 2026, Colorado employers, including local governments, will face new requirements and potential liabilities related to the use of AI in employment decisions under Senate Bill 24-205.



Accessibility Risks?

- Under Colorado's technology accessibility law, local governments are required to comply with statewide accessibility standards for individuals with a disability.
- The accessibility standards apply to both public external-facing and internal-facing information and communication technology (ICT)—such as software, applications, and websites—that is procured, developed, maintained, or used by local government entities.
- The law's broad coverage extends to third-party software forming part of a local government's ICT, and liability for noncompliance lies with the public entity that manages the content or platform/tool.
- The law's coverage extends to AI-tools and AI-generated content forming part of the local government's ICT!



Could Be A Public Record!

- With limited exceptions, prompts and AI-generated content are public records!
- Under CORA, "public records" are "all writings made, maintained, or kept" by local governments "for use in the exercise of functions required or authorized by law or administrative rule or involving the receipt or expenditure of public funds." C.R.S. § 24-72-202(6)(a)(I).
- Take steps to adequately address AI prompts and generated content in your records retention policies and be prepared to disclose them!
- Potential exceptions for deliberative process privilege and work product prepared for elected officials.
 - Prompts should not contain sensitive, personal, and confidential information, so exceptions to disclosure under CORA related to such information should not apply!



Risk Enhancers – "Shadow AI"

- Refers to the secret, unauthorized, or ungoverned use of AI tools.
- Poses risks to transparency, security, and decision-making.
- Potential legal issues related to the use of copyrighted information and inadvertent release of personal or sensitive information.
- Your organization should know about your employees' use of AI tools and how they're using it!
 - "This slideshow was prepared with assistance from ChatGPT and independently reviewed, researched, and fact-checked by the authors before publication. The authors take full responsibility for the content of this document."

□ Well, just the slides discussing ChatGPT hallucinations...but you get the point!

• Per HB 24-1147, Colorado has taken steps to require transparency—and impose liability—in one area of shadow AI: The use of "deepfakes" in candidate elections.



Risk Enhancers – AI Vendors

- Al tools used in local government are most often purchased from vendors as opposed to being developed by the local governments themselves.
- Use of AI tools developed by third parties heightens legal and liability risks because the local governments have less control over where their data is stored and how it is used.
- Vendor contracts typically heavily favor the vendor and may not recognize laws applicable to public entities.
- Risks increase even more when AI vendors contract separately with other parties to provide services in connection with the AI tool (e.g., third-party cloud storage; third-party AI widgets embedded in vendor software).
- It can be difficult to determine whether software purchased from a vendor includes third-party integrations, such as AI tools.
- Vendors are often unwilling to assume liability of third parties and defend/indemnify local governments against negligent acts and omissions of third parties.



External Cyber Threats

- Generative AI may introduce new or enhanced cyber vulnerabilities.
 - For example, generative AI has the potential to assist threat actors in engineering data breaches by producing sophisticated phishing emails, new types of malware capable of surpassing current cybersecurity protections, and computer code capable of exploiting system vulnerabilities without detection.
- Most of the mainstream generative AI platforms contain guardrails to prevent the generation of content that may assist in the commission of a crime and other unethical content.
- However, there are AI programs—sometimes referred to as "Unethical" or "Immoral" AI—that advertise a willingness to generate content without regard to the law or ethical concerns.



III. Suggestions For Safe & Efficient Use Of AI Tools

- Now that we've discussed various legal and liability risks involved, let's talk about what you can do to help your organization mitigate the risks and deploy AI tools safely and efficiently for your organization's benefit.
- To start, we suggest considering the following questions:
 - 1. What steps should we take *before* implementing AI tools? (Readiness)
 - 2. How do I evaluate AI tools for their benefits and risks? (Selection)
 - 3. What provisions should I seek to include in contracts for procurement/use of AI tools? (Contracting)



Readiness Suggestions (Part 1)

- Establish your local government's initial approach to AI—your "AI Culture."
 - How do we want to use AI? How does AI use align with your organization's mission statement and policy goals? Your commitment to constituents?
- Collaborate with other managers about their organizations' approach to Al and their Al uses.
- Develop an organization-wide policy for procurement of AI tools and acceptable AI use.
- Evaluate your organization's computing power, storage capacity, and networks to determine capacity for AI tools, and consider potential upgrades.
- Update cybersecurity practices and protections for AI threats.



Readiness Suggestions (Part 2)

- Appoint an AI coordinator or task force.
- Budget for AI experimentation.
- Pilot an AI tool start with something low risk, accessible, and that fits squarely within your organization's AI use policy (the pilot may help inform changes to your AI use policy!).
- Invest in AI training and educational resources for employees.
- Develop a mechanism/inventory for tracking your organization's data (third-party AI tools).
- Develop a mechanism for measuring AI impacts on your organization, good and bad.



Sample "Al Culture" Statements

- We embrace a culture of responsible AI experimentation where we maintain control and understanding of the use of AI tools in service to our residents.
- Our organization's use of AI is intended to support our work to deliver better, safer, more efficient, and equitable services to our residents.
- We understand that AI is a tool in service of our work, and that we are responsible for outcomes, good and bad, regardless of the tools we use to arrive at those outcomes.
- Our responsibility not to discriminate based on race, ethnicity, sex, religion, age, disability, veteran status, or other protected classifications, extends to our use of AI.
- We recognize that AI tools we use may impact on the security, privacy, and other rights of our constituents, and strive to protect those rights of our constituents through responsible use of AI tools.
- We will properly disclose and be transparent to the public about our use of AI tools and their impacts, good and bad.



Developing Your AI Policy

- Organization-wide policies for acceptable AI use and procurement should address, at minimum:
 - □ Statements as to your organization's culture, overarching principles, and approach to AI.
 - □ Appropriate uses, both general and specific to certain operations and specific job roles.
 - □ Prohibited uses (e.g., fully automated decisions without human oversight).
 - Establish risk categories for AI tool procurement; e.g., unacceptable, high, medium, low.
 - Provisions for protection of personal, sensitive, and confidential data (e.g., requirements for responsible user prompts).
 - $\hfill\square$ Provisions for compliance with applicable laws.
 - Mechanisms for *human* review of AI-generated content (for accuracy and bias and ensuring no copyrighted material is used without proper attribution/obtaining proper rights).
 - $\hfill\square$ Provisions for the security of login information and data.
 - □ Procedures for monitoring employee use and policy enforcement.
 - Organization/supervisory expectations for employee use of AI tools and transparency; e.g., employee disclosure of AI use (beware of "Shadow AI"!).
 - Provisions concerning the policy's interaction with other local government employment/IT policies.

Selecting AI Tools (Part 1)

• Consider these questions:

- □ How will the tool benefit my organization? (What are the rewards?)
- □ Will the tool bias our organization's decision-making (developer's point of view)?
- □ What is the tool's decision-making process? (How does the tool learn and generate content?)
- Does the AI tool explain its predictions, and how?
- □ What data has been used to train the tool? (Any copyrighted information?)
- What inputs does it need to produce useful outputs (personal, sensitive, confidential information)?
- What are the tool's performance metrics, and what's the tool's current performance as measured by those metrics?
- □ What conditions are necessary for the tool's optimal performance?
- □ Under what conditions does the tool perform poorly?
- What are the tools limitations?
- □ What is the tool's potential failure risk?

U What kind of errors can the tool make (e.g., hallucinations)?



Selecting AI Tools (Part 2)

• Questions (cont.):

- □ How can my organization monitor the tool's performance and potential failures?
- □ Does the tool include a way for my organization to review past system actions?
- Does the tool incorporate ways for my organization to report errors?
- $\hfill\square$ How often is the tool updated?
- □ Will my feedback be incorporated in updates?
- □ What bias does the tool's algorithm exhibit and how does it handle that bias?
- Does the tool/vendor comply with applicable laws (e.g., data privacy, accessibility, IP/copyright laws)? Our internal AI and IT policies?
- Does the tool incorporate adequate security features for the protection of data stored in the tool (inputs/outputs)?
- □ Will the vendor use our data inputs for other purposes not contemplated in the contract?
- Will my organization's data be shared with third parties? Which ones? If so, how does the vendor ensure the data's protection?

Consider creating a questionnaire to solicit responses from AI vendors!



Al Vendor Contracts (Part 1)

- Technology product vendor contracts typically heavily favor the vendor and may not recognize laws applicable to Colorado local governments.
- Vendors are often hesitant to negotiate substantive changes to their standard terms and conditions. But don't take no for an answer!
- Address the risks examined in this presentation!
 - Require the vendor to comply with applicable laws (e.g., data privacy, security, use rights; disability accessibility; IP/copyright infringement; high-risk AI).
 - Require the vendor to hold your organization harmless and defend/indemnify you against third-party claims and liabilities arising from the vendor's noncompliance with such laws, breaches of contract, and negligent acts and omissions.
 - Require the vendor to carry insurance of types/amounts sufficient to cover its indemnification obligations and to protect against risks arising from the vendor's work and the AI tool.
 - i.e., Tech professional E & O liability, general liability, and cyber risk insurance covering, among other things, developer negligence, security breach, data recovery, business interruption, cyber threats, infringement of intellectual property, privacy violations, release of PII, and other risks.
- Include provisions about what happens to your data when the contract ends (e.g. return & destroy!).

Al Vendor Contracts (Part 2)

- If your organization requires potential vendors to respond to a questionnaire, use it to inform potential revisions and additions to the vendor's contract. If possible, turn the responses into representations/warranties and include them in the contract.
- If your entity has an "incident response plan" related to technology security, consider attempting to bind the vendor to complying with it.
- Of course, work with your organization's attorney and IT department!



Scenario - AI Tool Selection & Vendor Contracting

Your organization is considering a software program developed by Rec-Intel, Inc. for use your recreation center that integrates two AI tools—each developed by a third party.

The first AI tool would fully automate customer account creation and take payments of membership fees. To set up membership accounts, customers must input their names, addresses, phone numbers, email addresses, and credit card information into the software, sign a general waiver & release, and create a unique username and password. The tool includes an option that allows recreation center employees to validate membership accounts before they go live but, according to the vendor, the option is unnecessary due to the software program's automation capabilities.

The second AI tool is a generative-AI chatbot that would assist customers with class bookings and other customer service items. The chatbot is trained on data provided by the recreation center, including a customer service FAQ document, and continuously retrains itself on customer interactions and feedback. The chatbot is supposed to notify recreation center employees when it cannot answer customer service questions or fulfill requests.

All customer information and chatbot data is stored on remote servers owned by a third party through a separate contract with the software vendor.



Al at the Rec. Center Scenario (Cont.)

- What do you want to know before you deciding to buy or pass?
- Should you exercise the "employee validation" option? Why?
- What provisions should you look for in the contract and seek to add if they're omitted?
- Hopefully, this presentation has provided a useful framework and resources to assist you in working though scenarios such as this one—and many others!



Concluding Thoughts

- Always remember: Al is a tool, and your organization is responsible for the outcomes of its tools. The technology is in service to your work and does not excuse your judgment or accountability.
- AI is a new and rapidly evolving field, and thus the potential policy impacts and risks to local government organizations are not fully known. Accordingly, local governments must keep a pulse on the changing landscape of opportunities and associated risks!
- Be transparent about your organization's use of AI—internally and publicly!
- Involve your organization's attorney and IT department at the policymaking, procurement, and contracting stages of AI implementation.
- If you're a CIRSA member, know we are here to help you as you delve into the exciting world of Artificial Intelligence!



Resources

- CIRSA, Embracing the Future: Responsible Use of Generative Artificial Intelligence in Local Government Operations: https://www.cirsa.org/blog/embracing-the-future-responsible-use-of-generative-artificial-intelligence-in-local-government-o-generations/
- CIRSA, *Mitigating Risk In Local Government Technology Contracts:* <u>https://www.cirsa.org/blog/mitigating-risk-in-local-government-technology-contracts/</u>
- CML, Harnessing the Benefits and Managing the Risks of Artificial Intelligence in Municipal Government, Jan. 26, 2024 CML Newsletter:
 - https://www.cml.org/docs/default-source/cml-newsletter/cml-newsletter-2024-26-1.pdf?Status=Temp&sfvrsn=17131f9f_2
- State of Colorado Statewide GenAl Policy: <u>https://servicehub.colorado.gov/ts?id=tech_standard&sysparm_article=KB0012606</u>
- City of Boston Interim Guidelines for Using Generative AI: <u>https://mrsc.org/getmedia/2e12163d-e556-42c8-80b3-b6f2cd41c02f/m58Bgaipol.pdf</u>
- GovAI Coalition: Artificial Intelligence Templates and Resources (factsheets, template policies, vendor agreements, etc.): <u>https://www.sanjoseca.gov/your-government/departments-offices/information-technology/artificial-intelligence-inventory/g</u> <u>ovai-coalition/templates-resources</u>
- Municipal Resources and Services Center (MRSC), Use of Generative AI by Local Governments: <u>https://mrsc.org/stay-informed/mrsc-insight/july-2023/use-of-generative-ai-by-local-governments</u>
- University of Michigan & Michigan Municipal League, Artificial Intelligence Handbook for Local Government: <u>https://mml.org/wp-content/uploads/2024/11/AI-Handbook-UM-and-MML-2024.pdf</u>



About the Colorado Intergovernmental Risk Sharing Agency (CIRSA)

- Public entity self-insurance pool for property, liability, and workers' compensation coverages
- Formed by in 1982 by 18 municipalities pursuant to CML study committee recommendations
- Not an insurance company, but an entity created by intergovernmental agreement of our members
- Total membership today stands at 293 member municipalities and affiliated legal entities
- Member-owned, member-governed organization
- No profit motive sole motive is to serve our members effectively and responsibly
- CIRSA Board made up entirely of municipal officials
- Seek to be continually responsive to the liability-related needs of our membership coverages and associated risk management services, sample publications, training, and consultation services, as well as specialty services such as home rule charter review
- We have the largest concentration of liability-related experience and knowledge directly applicable to Colorado municipalities



Speaker Bios

Sam Light is Deputy Executive Director/General Counsel for CIRSA. Prior to joining CIRSA in 2018, he was a partner with the Denver law firm of Light | Kelly, P.C., specializing in municipal and other public entity law, insurance law, and defense of public entities and elected officials. Sam has over 25 years of experience serving as general or special counsel to several Colorado cities, towns, self-insurance pools, and other public entities, and he is a frequent speaker on public entity risk issues.

Nick Cotton-Baez is Associate General Counsel for CIRSA. Nick is a frequent speaker on public entity risk and legal issues and has practiced law in Colorado since 2016. Before joining CIRSA, Nick previously worked in the Denver City Attorney's Office, and then for a full-service municipal law firm, where he served as general and special counsel for municipalities, self-insurance pools, and other public entities throughout Colorado.

Note: The suggestions in this presentation are those of the authors, who takes full responsibility for them...any resemblance strictly coincidental, etc. This presentation is a training resource only and not legal advice. In the event of any conflict between training tips and the advice of your entity's attorney, the advice of your attorney prevails!