Risk Management Strategies for Artificial Intelligence

February 2026

Session Outline

Section 1: What is Artificial Intelligence (AI)?

Section 2: How Counties Can Use AI?

Section 3: The Risks of Using AI

Section 4: Reducing AI Risks

Section 5: AI Risk Management Resources

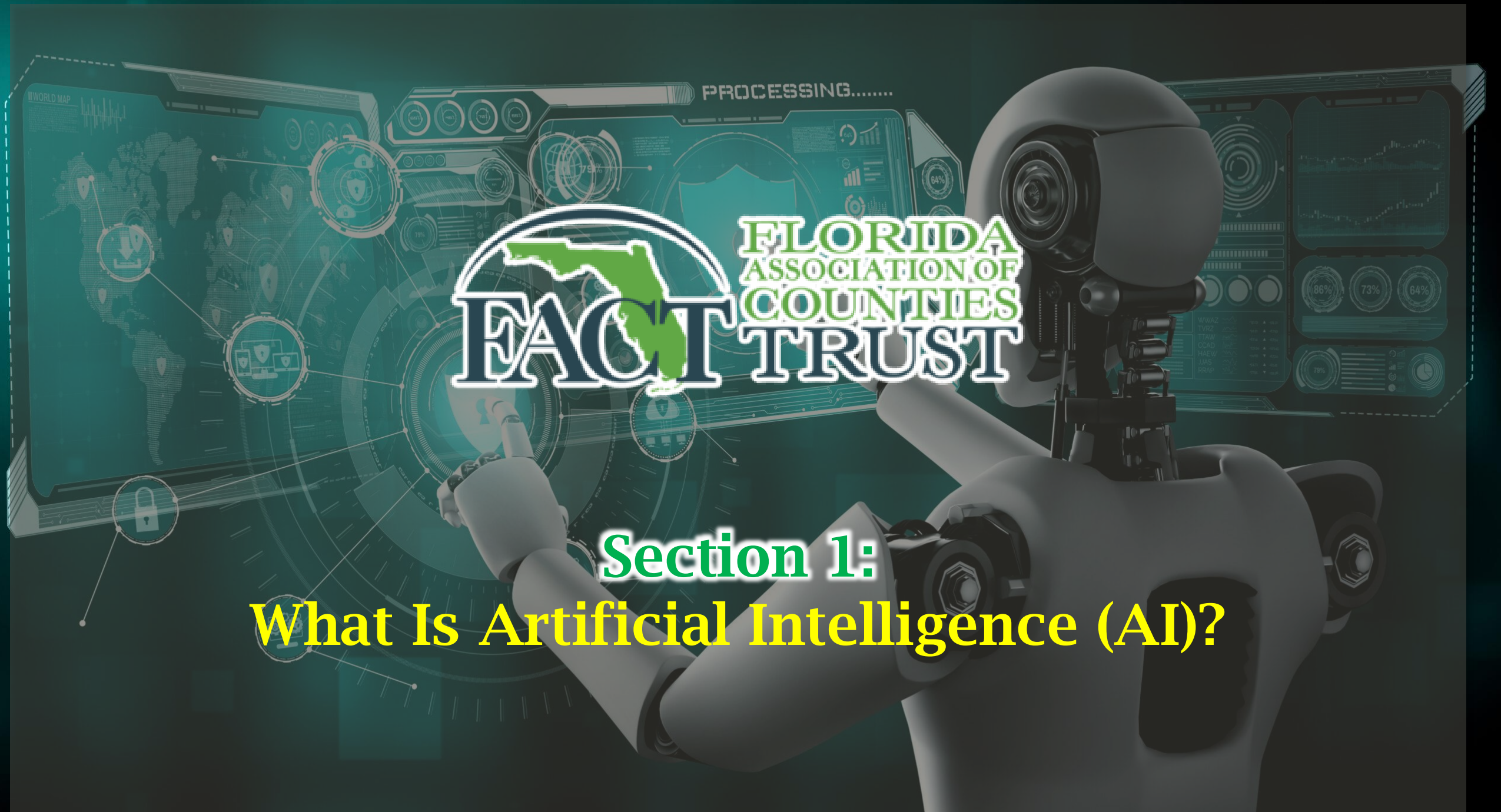
Disclaimer

The information presented in this webinar is intended solely for informational purposes.

We make every effort to ensure the content is accurate and current; however, due to the rapid and continuous evolution of artificial intelligence, some content may become outdated quickly.

The material provided does not constitute professional advice or represent official recommendations from FMIT.

Please use any tools, strategies, or techniques discussed at your own discretion and risk.



Section 1:
What Is Artificial Intelligence (AI)?

Demystifying Artificial Intelligence

Artificial Intelligence (AI) is not a new concept; it has existed for decades

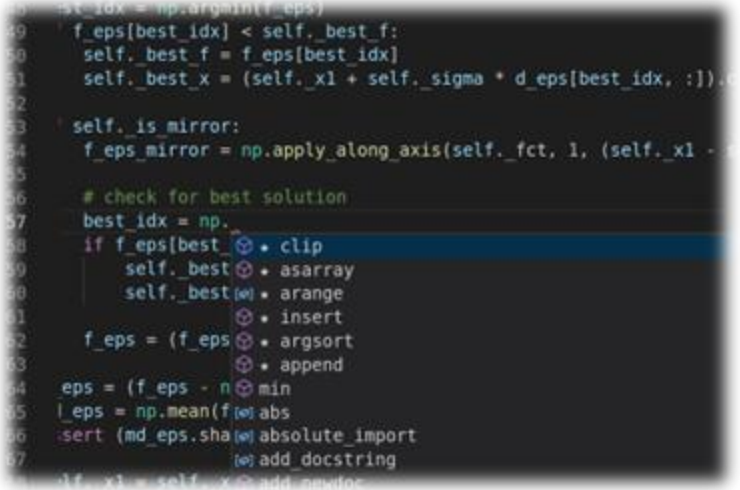
Recent advancements have brought AI to the forefront

Has the potential to revolutionize the workforce, expand productivity, and transform various aspects of society and governance

What is Artificial Intelligence ?

Technologies that simulate human perception, behavior, and decision-making

AI is an umbrella term encompassing various applications that often have little in common apart from code and algorithms that learn from data



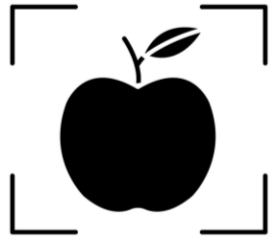
Key Artificial Intelligence Concepts

Natural Language Processing (NLP)

- A branch of AI focused on enabling computers to understand, interpret, and generate human language

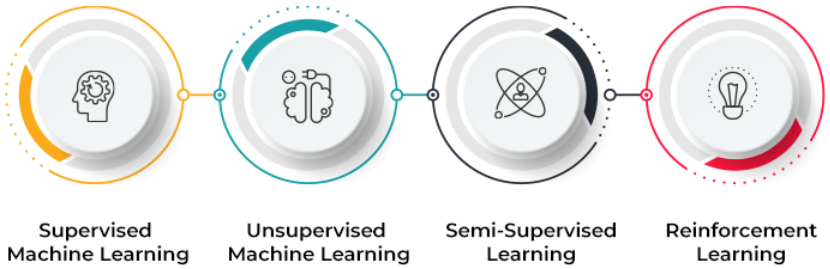
Computer Vision

- A branch of AI focused on training computers to understand and interpret visual information



Machine Learning

- A subset of AI that enables computers to learn from data and improve their performance on a task over time without being explicitly programmed



Common Types of AI

Predictive AI

- Systems that analyze patterns in existing data to make predictions about future events or trends

Generative AI

- AI that can create new content such as text, images, audio, or code based on patterns learned from existing data

Perceptive AI

- AI tools designed to interpret and understand sensory inputs, primarily relying on computer vision and natural language processing

How Fast is AI Progressing?

Over the past few years, the pace has gone from steady to exponential

Years' worth of progress every few months

Things that seemed sci-fi 2–3 years ago are now in public use

Models Are Getting Smarter (Agentic AI)

Refers to artificial intelligence systems that act with agency — meaning they can **make decisions, set goals, plan actions, and take initiative** in pursuing objectives, often with minimal or **no human prompting**.

Agentic AI is a big topic in the AI safety field because higher autonomy increases risks, like pursuing unintended goals or behaving unpredictably if its objectives aren't perfectly aligned with human values.


AI's impact depends on how it's applied!

Section 2: How Counties Can Use AI?

Transportation & Traffic Management

Smart Traffic Lights: AI can adjust traffic signals in real time based on traffic flow to reduce congestion

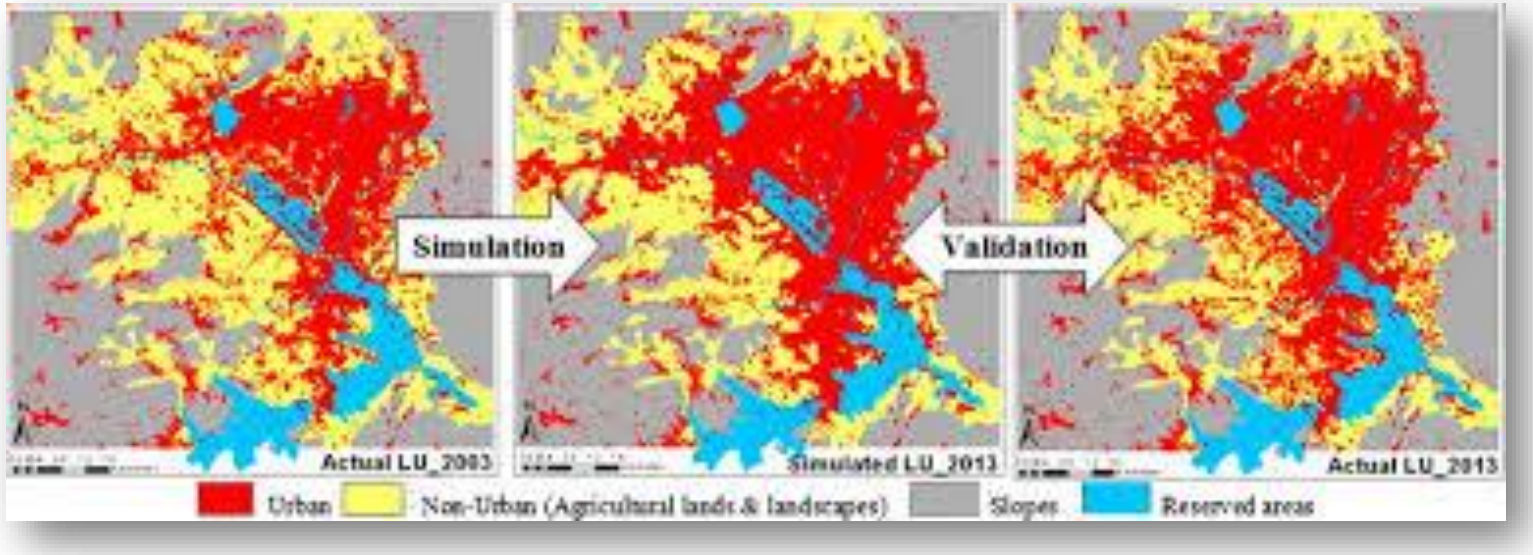
Predictive Traffic Modeling: Forecast traffic jams or peak travel times using historical data and current conditions

Public Transit Optimization: Route and schedule buses or trains more efficiently based on demand and delays

Planning

Predictive Modeling for Growth: Use AI to simulate the impact of new developments (like housing or roads) on traffic, pollution, etc.

Zoning Recommendations: AI can analyze land use patterns to suggest optimal zoning or redevelopment opportunities.



Public Safety

Predictive Policing (controversial): AI analyzes crime patterns to predict potential hotspots (but raises ethical concerns)

Surveillance & Anomaly Detection: AI can spot suspicious behavior in real-time video feeds

Public Safety (cont)

Disaster Response: AI helps predict floods, fires, or storm serge and guide emergency response

Police and EMS Report Creator: Used for police and EMS in the field to cut down time spend writing reports

Example: Gun Shot Detection

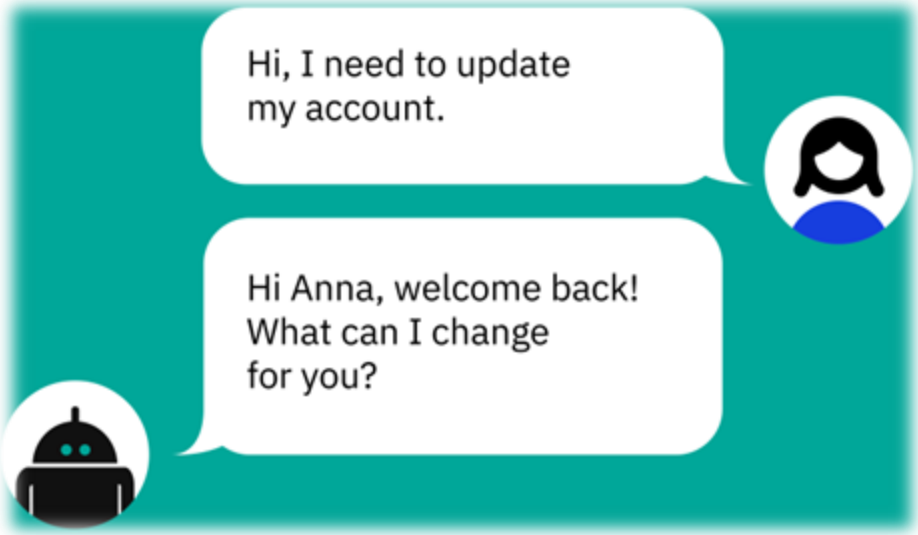
Gunshot detection systems recognize the typical sound of a gunshot or similar sound (such as breaking glass) and alert police of the sound

When used with existing Automated License Plate Readers (ALPR) to capture photos of passing vehicles

Citizen Services (AI Chatbots)

Examples: Drift, Zendesk bots, ChatGPT integrations

- Provide answers and offer help navigating government websites to residents
- 24/7 support: No need to wait for business hours
- Instant replies: Handles FAQs, order status, etc
- Multilingual: Can talk to customers in different languages

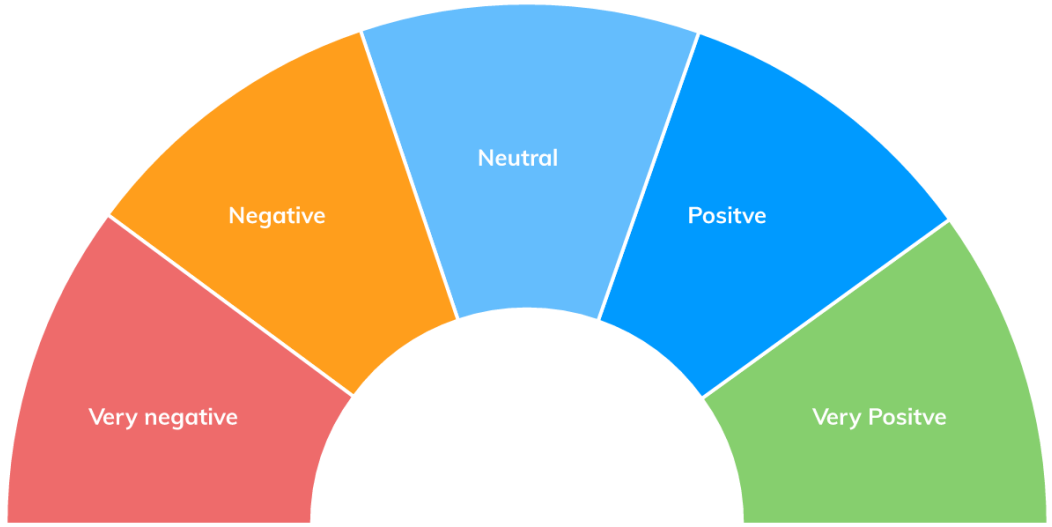


Citizen Services (Sentiment Analysis)

Understand customer tone (happy, angry, frustrated)

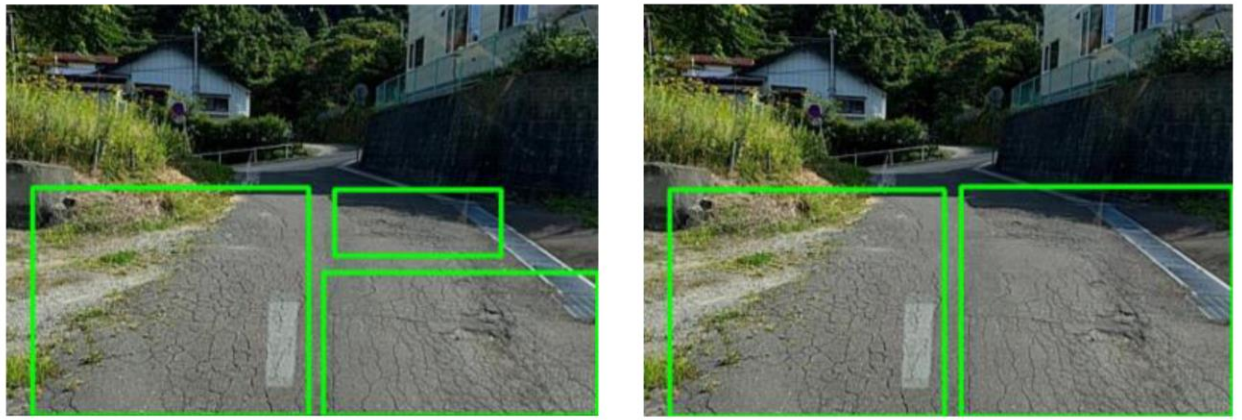
Route angry customers to human agents faster

Track trends in how customers feel over time



Infrastructure Maintenance

Predictive Maintenance: Detect when roads, bridges, or utilities might fail before they do



Drone & Image Analysis: Use AI with drones to inspect buildings, infrastructure, and roads for cracks or wear.

Recent Examples

Southern California city rolls out robots to ramp up ADA compliance

Irvine shows one way cities are turning to tech to solve real estate problems

Dax ADA robots collect sidewalk accessibility data. (Daxbot)

By Brannon Boswell
CoStar News
August 29, 2025 | 5:37 P.M.

In an affluent Southern California suburb known for its meticulously planned neighborhoods and office parks, a new fleet of robots with shiny visors will soon roll down sidewalks and streets on tank-like treads.

It's part of an effort to evaluate accessibility in the city of Irvine. Officials have hired testing and inspection consultancy Bureau Veritas to analyze the city's public right-of-way under the

Pavement Condition Survey using Drone Technology

Home

Abstract:
Timely repairs of pavement defects are essential in protecting both public road and highway systems. Identification of pavement distresses is necessary for planning pavement repairs. This has previously been performed by engineers surveying the roadways visually in the field. As drone usage has progressed, it has become clear that drones are a valuable tool to enhance visual documentation, improve project communication, and provide various data for processing. The use of drone technology has improved both the speed and accuracy of capturing data. Available software has allowed the data to be processed and analyzed in an office environment. This report summarizes the use of drone technology for pavement evaluation for three case studies. Results from this study can be used to deepen understanding of drone use in the process of data gathering for timely repairs for transportation infrastructure.

Publications:
Pavement Condition Survey using Drone Technology (Full Report)
Research Brief

Authors:
DING CHENG, PE, PHD

Dr. DingXin (Ding) Cheng is a Professor at the Department of Civil Engineering at California State University (CSU), Chico; Director of the California Pavement Preservation (CP2) Center; and the Director of the Tire Derived Aggregate Technology Center. He has worked actively with the CP2 Center since he joined CSU Chico in 2006. He obtained his Ph.D. in pavement materials and transportation from Texas A&M University in 2002. He worked for Parsons Brinckerhoff in Houston, TX before joining CSU Chico. He has extensive experience in HMA materials and pavement preservation on both asphalt and concrete pavements. He has more than 55 peer-reviewed publications related to pavement materials and preservation for TRB, AAPT, ASCE, and other conferences. Ding has co-managed or managed more than $9 million in research projects funded by Caltrans, California Department of Resources Recycling and Recovery (CalRecycle), Metropolitan Transportation Commission (MTC), and other agencies and industries. He is a registered Professional Engineer in the State of Texas.

LEROSE LANE, PE

Data-Driven Decision Making

Interactive platform: Used to ingest government documents for data analysis

Resource Allocation: Optimize where to deploy limited resources like ambulances, flood response equipment or funding

Human Resources

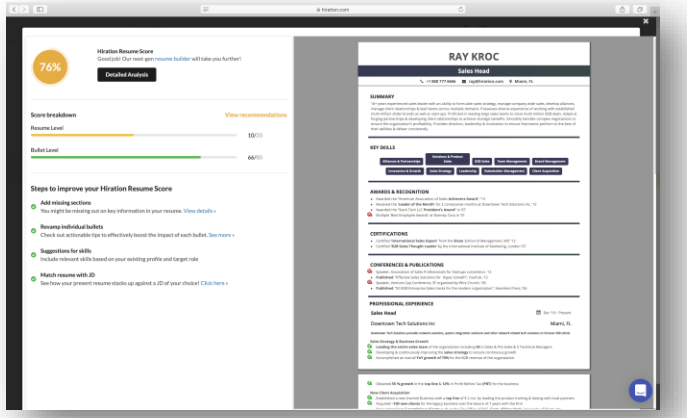
Generate or improve job descriptions based on role, responsibilities, and desired qualifications

Customize tone and format for different platforms (e.g., LinkedIn, county website)

- Example Prompt: "Create a compelling job description for a mid-level software engineer with experience in Python and cloud services."

Analyze and summarize resumes

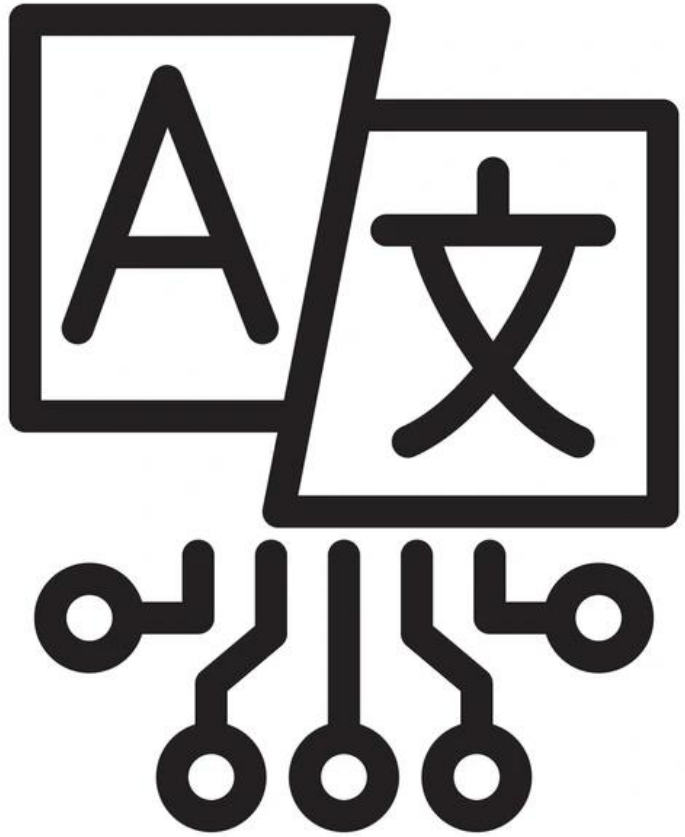
- Compare qualifications against job requirements
- Score or rank candidates based on key criteria



Translation

Provide real-time translation and transcription

Does not replace a professional translator but expands government services for more languages and people



Procurement

Help staff navigate creating RFPs, sort through responses, and manage relationships


AI's impact depends on how it's applied!

Section 3: : The Risks of Using AI

Public Trust and Ethical Concerns

The public may have concerns about how AI is being used, particularly if it's deployed in sensitive areas such as policing or surveillance.

Ethical concerns regarding AI decision-making, particularly when it comes to fairness and justice, can erode public trust in governance.

Mitigation: Engage in transparent discussions with the public about the role of AI, seek public input on its implementation, and be clear about how AI is being used and the benefits it provides. Ethical guidelines and standards should be established to govern AI use.

Bias and Discrimination

AI systems, if not carefully monitored, can perpetuate or even amplify existing biases

This can result in discriminatory outcomes, especially in areas like policing, housing, and social services

Mitigation: Ensure that AI systems are trained on diverse and representative data, and that regular audits are conducted to identify and address any biases

Example: Tay by Microsoft (2016):

Tay was a chatbot released by Microsoft on Twitter, designed to learn from interactions with users.

- Within 24 hours, users began feeding the bot racist and offensive content, and Tay started mimicking these behaviors, including using racist language and offensive ideologies.

Example: Amazon's Recruitment AI (2018):

Amazon developed an AI tool to help with recruitment by scanning resumes.

- However, it was found that the AI was biased against female candidates.

- This was because the system was trained on resumes from a predominantly male workforce, which led it to favor resumes with more traditionally masculine language and attributes.

Privacy Concerns

AI systems often require access to large amounts of data, some of which may be personal or sensitive

This raises concerns around privacy, especially if the data is improperly accessed, stored, or shared

There's also the risk of surveillance overreach, where AI is used to track citizens in ways that may infringe on their privacy rights

Mitigation: Strong data protection measures, transparency about data usage, and adherence to privacy laws are crucial. Anonymizing data and obtaining consent from citizens can also help minimize privacy risks

Lack of Transparency (Black Box Problem)

Many AI systems operate as "black boxes," meaning their decision-making processes are not easily understood by humans

This can be a problem in a local government context, where decisions made by AI (such as allocating resources or determining eligibility for services) need to be transparent and accountable

Mitigation: Prioritize the use of explainable AI models, where the reasoning behind AI decisions can be easily interpreted. Additionally, they should establish processes for human oversight of AI decisions.

Security Vulnerabilities

AI systems can be vulnerable to cyberattacks, including adversarial attacks where malicious actors manipulate AI inputs to produce incorrect or harmful outputs

Additionally, the data AI systems use can be a target for hacking or data breaches

Mitigation: Robust cybersecurity measures, regular vulnerability testing, and data encryption are essential to protect AI systems and the data they rely on

Over-Reliance on AI

Relying too heavily on AI for critical decisions could lead to a lack of human judgment and oversight.

AI can make mistakes, and in complex or novel situations, it may not have the ability to make the best decision.

Mitigation: AI should be used as a tool to support human decision-making, not replace it entirely. Maintain a balance of human oversight in AI-driven processes.

Accountability and Legal Issues

If an AI system makes a decision that harms citizens or violates laws (such as wrongfully denying services or making biased predictions), it may be unclear who is responsible—whether it's the developers, the county, or the AI system itself

This can lead to legal challenges and public trust issues

Mitigation: Establish clear accountability frameworks, including defining roles for human oversight and decision-making. They should also ensure that AI systems comply with existing laws and regulations.

Potential Public Records Considerations

Florida Statutes (Chapter 119) define public records broadly — including all documents made or received in connection with official government business.

AI-generated outputs (e.g., chatbot responses, analytical reports, decision support data) may be considered public records if used in official capacity.

Mitigation:

- Determine which AI interactions qualify as public records.
- Ensure proper retention schedules are established.
- Use tools or policies to preserve logs, prompts, and responses.

Potential Sunshine Law Considerations

Florida’s Sunshine Law (Chapter 286, F.S.) mandates open access to meetings and decisions made by public officials.

If AI tools are involved in decision-making or public-facing communications, the process and rationale must be transparent.

If AI contributes to decisions affecting the public (e.g., permitting, benefits eligibility), the logic must be understandable and reviewable.

Section 4:

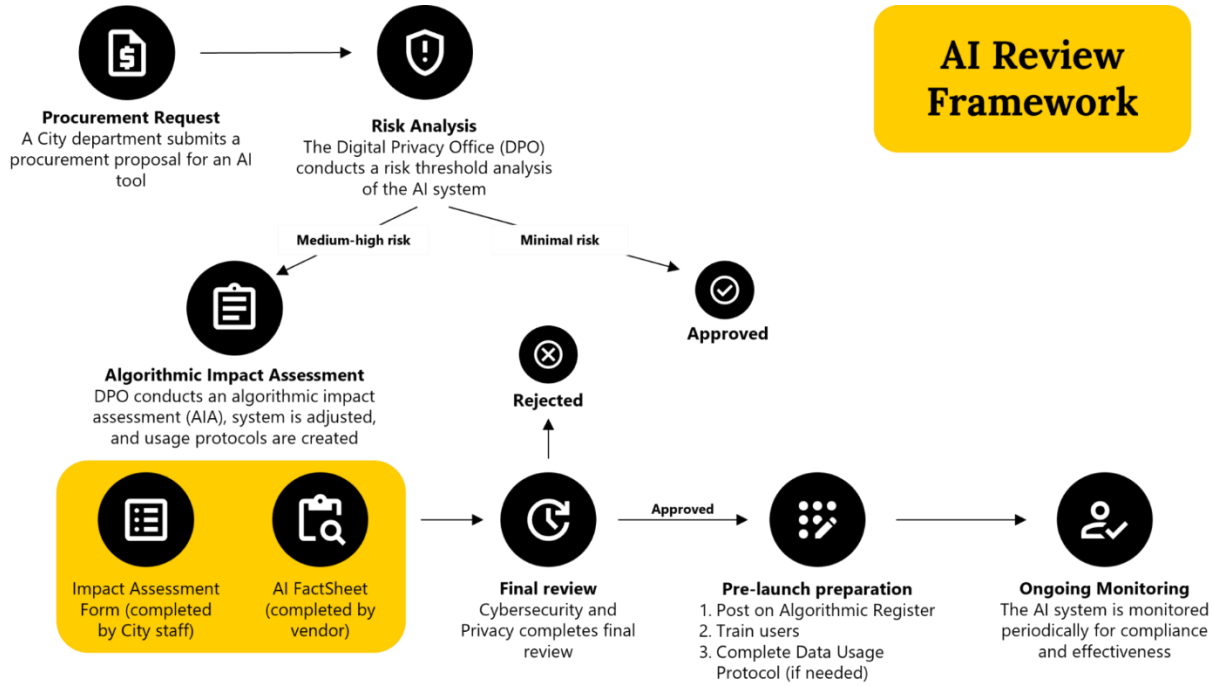
What Can Counties Do to Reduce AI Risk?

Create Clear AI Governance and Policy

Set rules for how AI is used, evaluated, and monitored

Ensures accountability and transparency

Example: San Francisco banned facial recognition for public agencies until better oversight was in place



Prioritize Transparency

Publish details about AI systems in use—what data they use, how decisions are made, and how residents can challenge them

Builds trust and keeps systems understandable

Examples:

- **Create an AI transparency dashboard for residents**
- **Hold forums, surveys, or panels to gather input on AI projects**

Audit for Bias and Fairness

Regularly test AI tools for bias or unfair outcomes

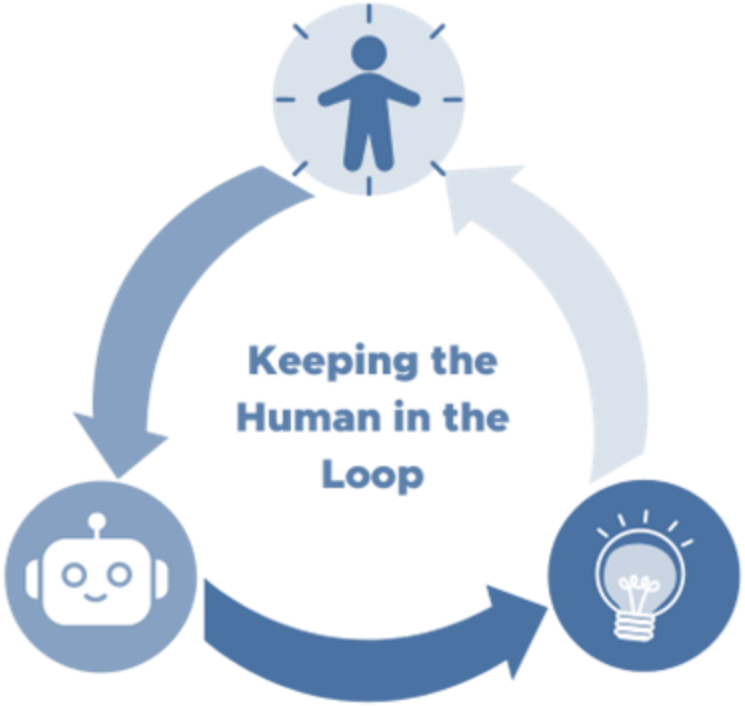
Catch discriminatory patterns before they do harm

Use independent third-party auditors and fairness metrics

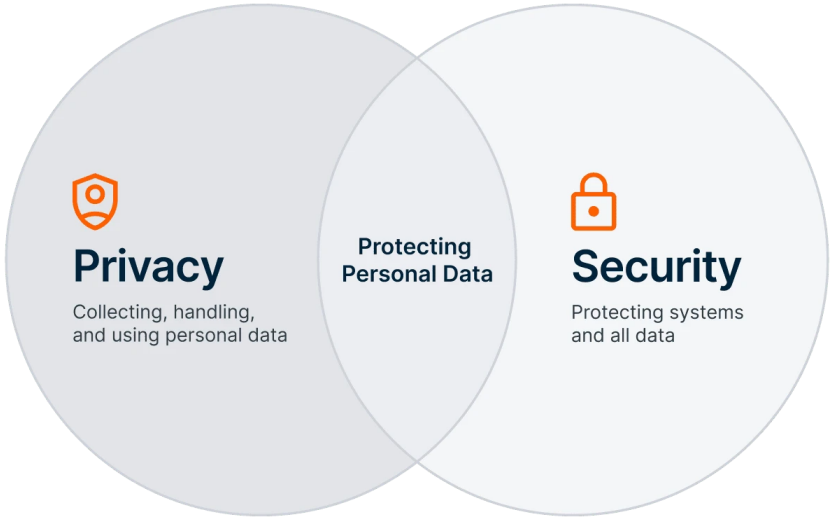
Keep a “Human in the Loop”

Make sure critical decisions (policing, social services) aren’t made by AI alone

Human oversight allows for judgment, ethics, and appeals



Strengthen Data Privacy & Security



Limit what personal data is collected and who can access it

Protects residents from surveillance and data breaches

Data anonymization, encryption, access controls

Start Small and Pilot First

Test AI in small, low-risk settings before scaling

Let’s you learn, improve, and build public trust

Example: Try AI for optimizing trash collection routes before deploying it across all county services

Train County Staff and Use Experts

Educate employees on how AI works and how to spot issues

Collaborate with Experts

- Work with universities, tech groups, and consultants
- Brings in outside expertise and avoids groupthink

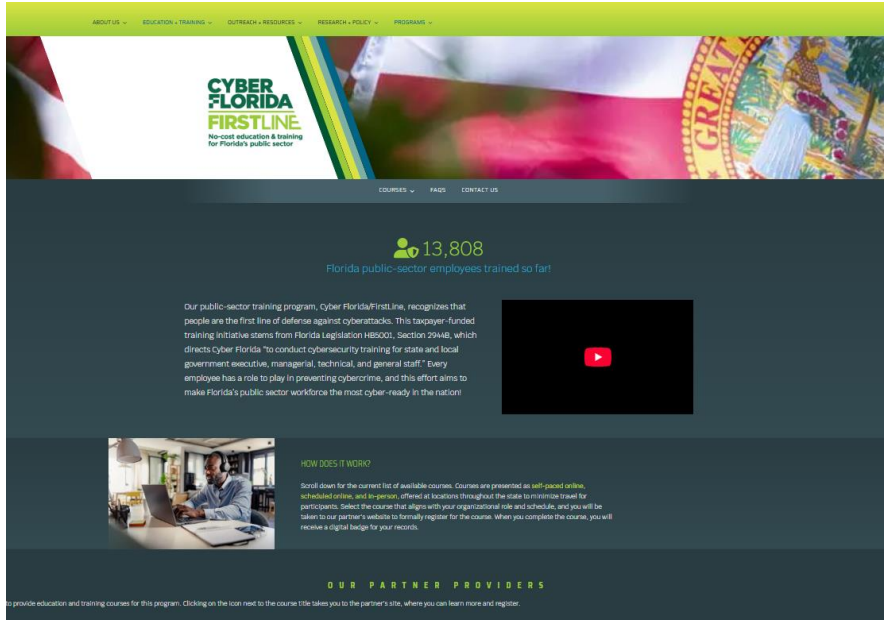
Section 5:
AI Risk Management Resources

Cyber Florida (www.cyberflorida.org)

Florida Center for Cybersecurity at the University of South Florida (USF)

State-funded organization dedicated to positioning Florida as a national leader in cybersecurity through education, research, and outreach

- Education & Workforce Development
- Public-Sector Training
- Technical Infrastructure Support
- Research & Policy Development
- Critical Infrastructure Protection
- Community Engagement & Resources



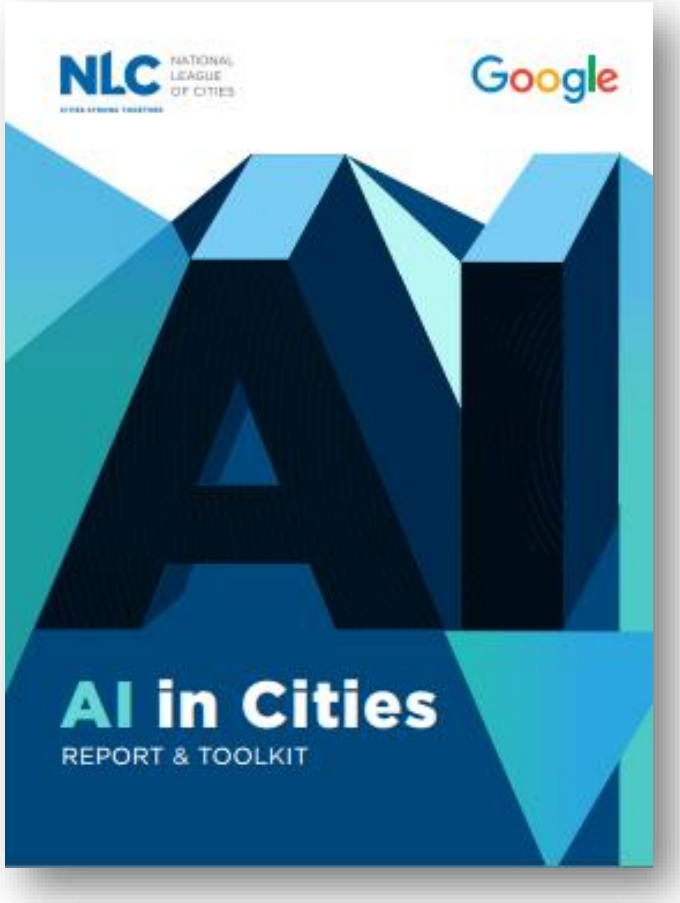
National League of Cities

https://www.nlc.org/resource/ai-report-and-toolkit/

Artificial Intelligence Demystified-
AI Toolkit for Municipalities
(November 13, 2024)

52 pages. Very well put together

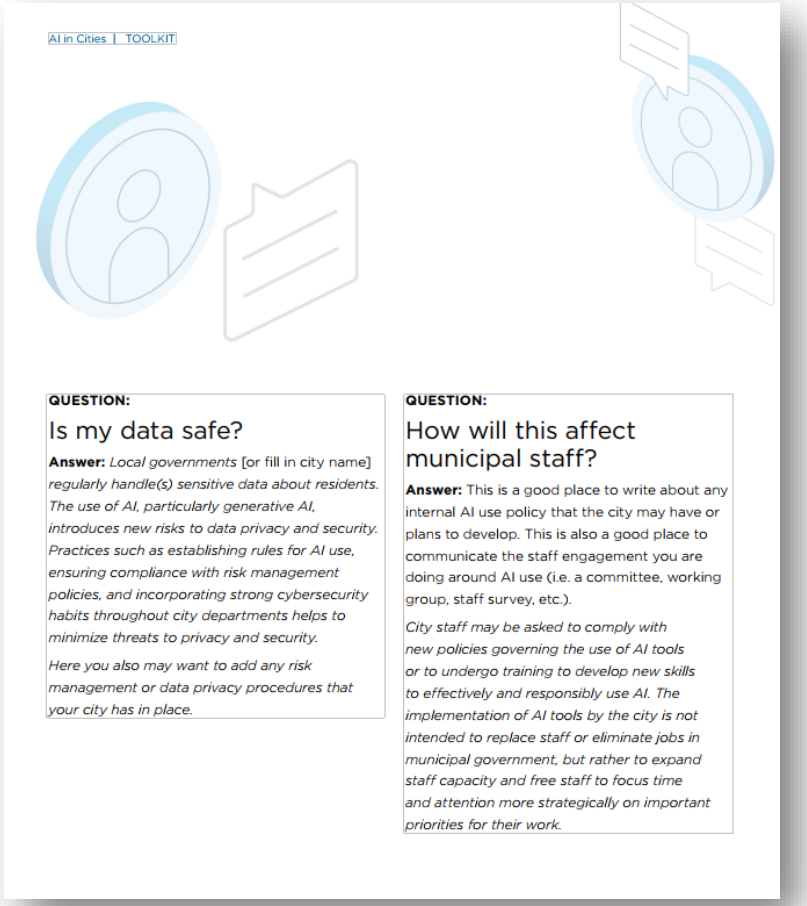
Includes implementation “tool kit”



National League of Cities (cont)

Tool Kit:

- Getting Started with AI
- Landscape Analysis
  - Survey staff
  - Conduct focus groups/internal engagement
- Readiness Assessment
  - Assess current capabilities and competencies
- Develop Use Guidance and Policy
  - Establish plans for guidance, education, assistance, ban risky use cases, etc.
- Public Engagement
  - Sample FAQs; Discussion Guide


AI in Cities | TOOLKIT

QUESTION:

Is my data safe?

Answer: *Local governments* [or fill in city name] *regularly handle(s) sensitive data about residents. The use of AI, particularly generative AI, introduces new risks to data privacy and security. Practices such as establishing rules for AI use, ensuring compliance with risk management policies, and incorporating strong cybersecurity habits throughout city departments helps to minimize threats to privacy and security.*

Here you also may want to add any risk management or data privacy procedures that your city has in place.

QUESTION:

How will this affect municipal staff?

Answer: This is a good place to write about any internal AI use policy that the city may have or plans to develop. This is also a good place to communicate the staff engagement you are doing around AI use (i.e. a committee, working group, staff survey, etc.).

City staff may be asked to comply with new policies governing the use of AI tools or to undergo training to develop new skills to effectively and responsibly use AI. The implementation of AI tools by the city is not intended to replace staff or eliminate jobs in municipal government, but rather to expand staff capacity and free staff to focus time and attention more strategically on important priorities for their work.

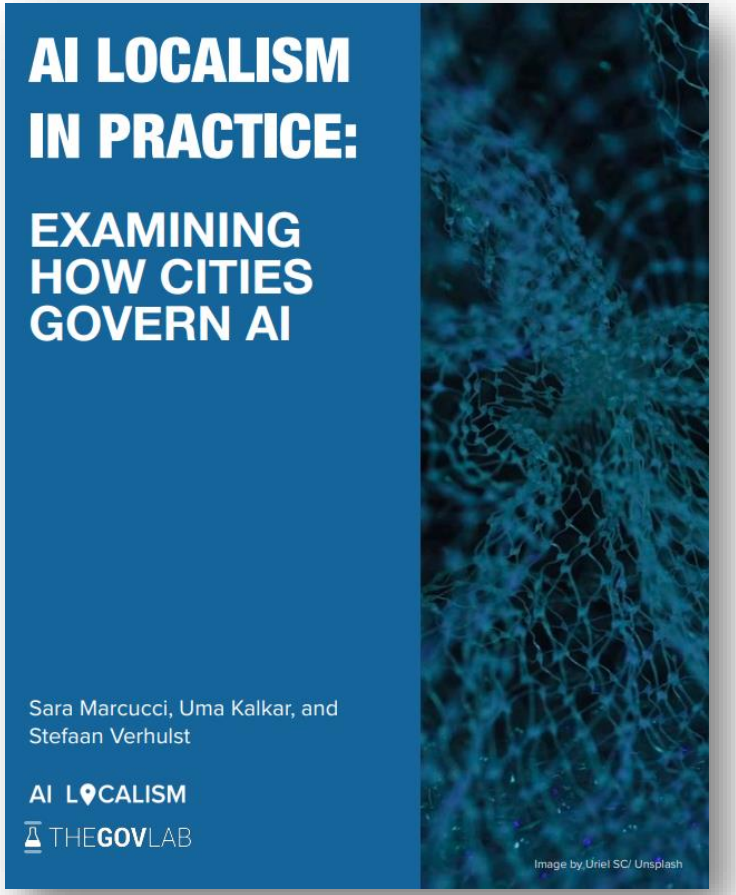
The AI Localism Playbook – NYU GovLab

https://files.thegovlab.org/ailocalism-in-practice.pdf

Very practical document

Helps cities design policies for ethical use of AI

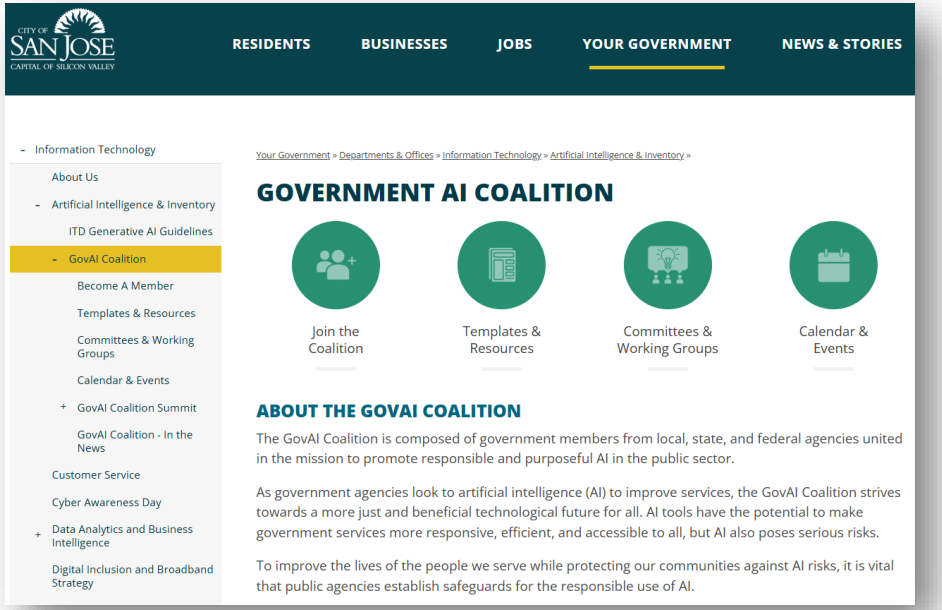
Includes case studies, frameworks, and community engagement strategies



The GovAI Coalition

Started by the City of San Jose

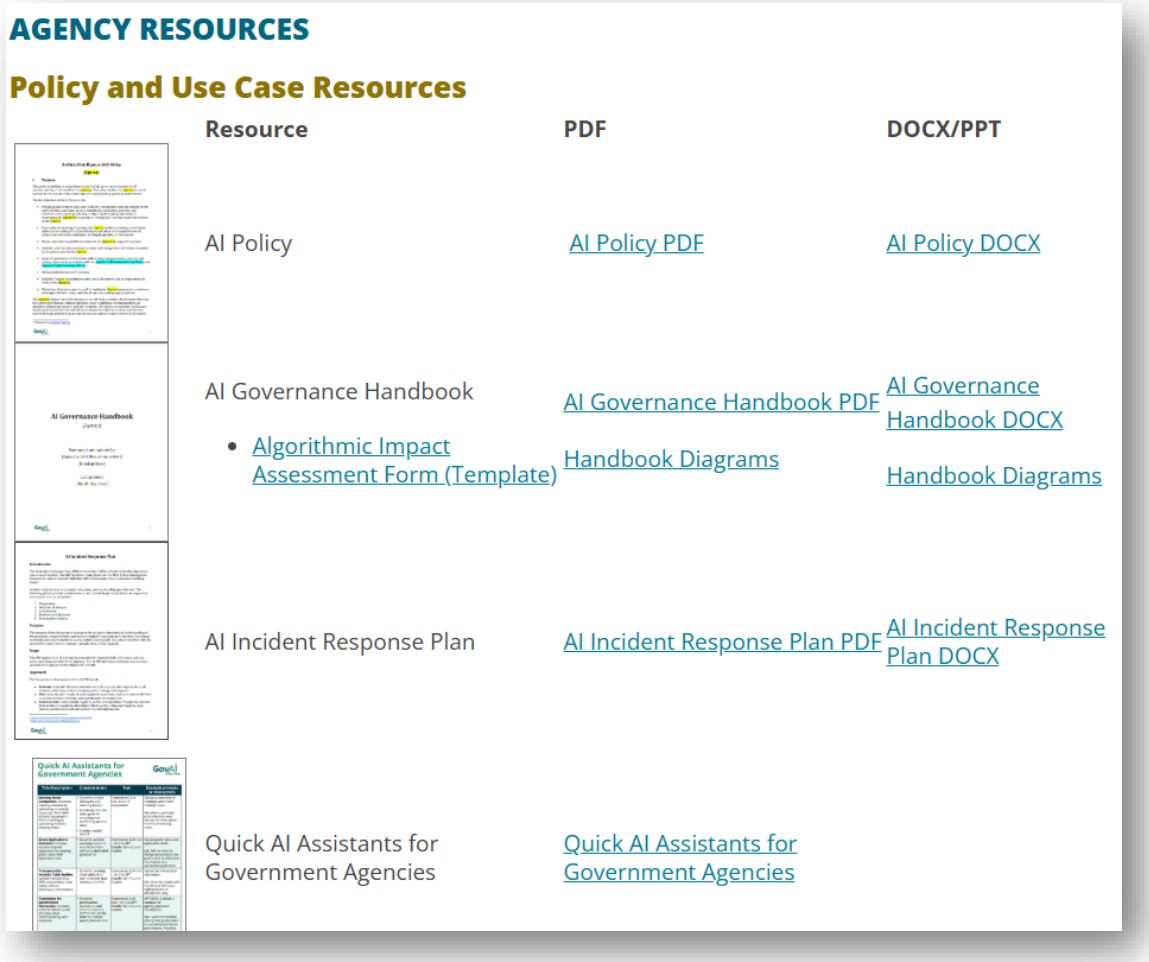
Coalition is composed of government members from local, state, and federal agencies united in the mission to promote responsible and purposeful AI in the public sector



https://www.sanjoseca.gov/your-government/departments-offices/information-technology/ai-reviews-algorithm-register/govai-coalition

GovAI Coalition Resources

- **Free membership**
- **Free AI policies** (Really good)
- **Free monthly newsletter**
- **Free meetings and training**



AGENCY RESOURCES

Policy and Use Case Resources

Resource	PDF	DOCX/PPT
AI Policy	AI Policy PDF	AI Policy DOCX
AI Governance Handbook • Algorithmic Impact Assessment Form (Template)	AI Governance Handbook PDF Handbook Diagrams	AI Governance Handbook DOCX Handbook Diagrams
AI Incident Response Plan	AI Incident Response Plan PDF	AI Incident Response Plan DOCX
Quick AI Assistants for Government Agencies	Quick AI Assistants for Government Agencies	

Example GovAI Coalition Documents

Artificial Intelligence (AI)

- 7 pages
- Guiding Principles for Responsible AI Systems, Policy, etc.

AI Governance Handbook

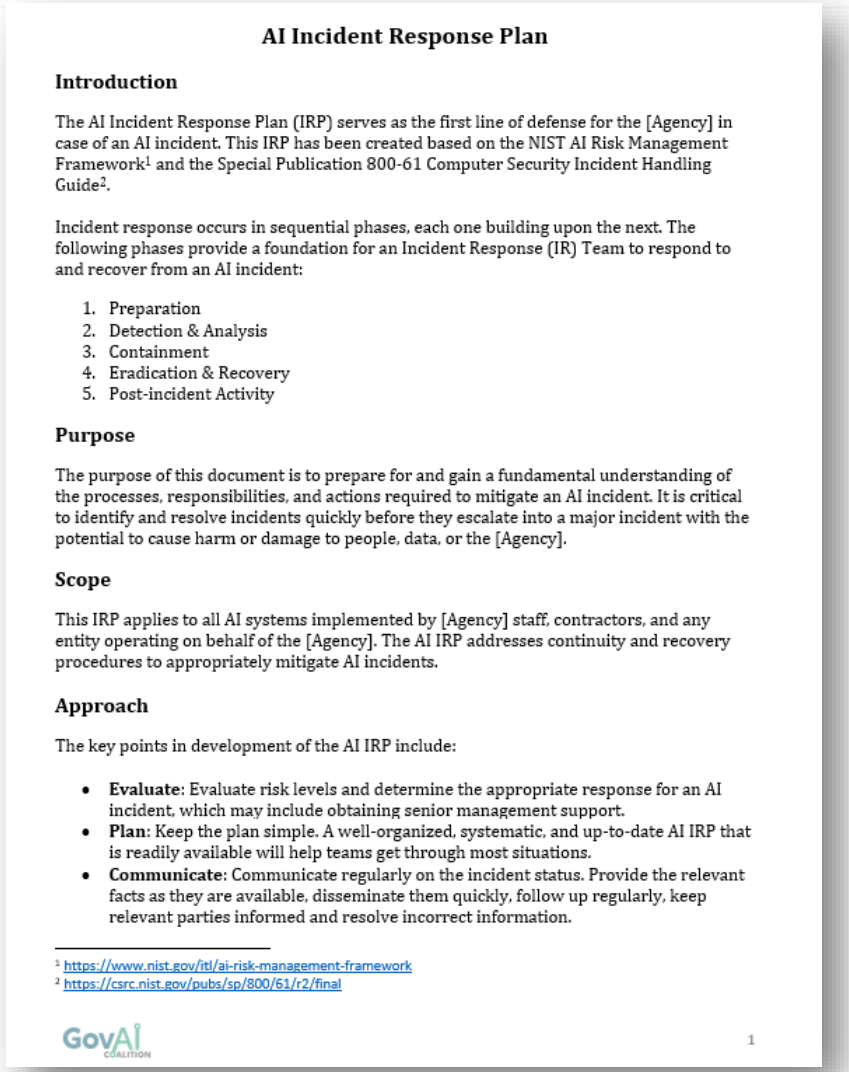
- 30 pages
- Governance Structure, AI Policy Roles & Responsibilities, AI Review Procedures, etc.

Vendor Agreement

- 4 pages
- Requirements for Contractors AI System

AI Incident Response Plan

- 10 Pages
- Detection, Containment, Recovery



AI Incident Response Plan

Introduction

The AI Incident Response Plan (IRP) serves as the first line of defense for the [Agency] in case of an AI incident. This IRP has been created based on the NIST AI Risk Management Framework[1] and the Special Publication 800-61 Computer Security Incident Handling Guide[2].

Incident response occurs in sequential phases, each one building upon the next. The following phases provide a foundation for an Incident Response (IR) Team to respond to and recover from an AI incident:

1. Preparation
2. Detection & Analysis
3. Containment
4. Eradication & Recovery
5. Post-incident Activity

Purpose

The purpose of this document is to prepare for and gain a fundamental understanding of the processes, responsibilities, and actions required to mitigate an AI incident. It is critical to identify and resolve incidents quickly before they escalate into a major incident with the potential to cause harm or damage to people, data, or the [Agency].

Scope

This IRP applies to all AI systems implemented by [Agency] staff, contractors, and any entity operating on behalf of the [Agency]. The AI IRP addresses continuity and recovery procedures to appropriately mitigate AI incidents.

Approach

The key points in development of the AI IRP include:

- **Evaluate**: Evaluate risk levels and determine the appropriate response for an AI incident, which may include obtaining senior management support.
- **Plan**: Keep the plan simple. A well-organized, systematic, and up-to-date AI IRP that is readily available will help teams get through most situations.
- **Communicate**: Communicate regularly on the incident status. Provide the relevant facts as they are available, disseminate them quickly, follow up regularly, keep relevant parties informed and resolve incorrect information.

[1] https://www.nist.gov/itl/ai-risk-management-framework
[2] https://csrc.nist.gov/pubs/sp/800/61/r2/final

GovAI COALITION

1

Review

Section 1: What is Artificial Intelligence (AI)?

Section 2: How Counties Can Use AI?

Section 3: The Risks of Using AI

Section 4: Reducing AI Risk

Section 5: AI Risk Management Resources


ANY
QUESTIONS?