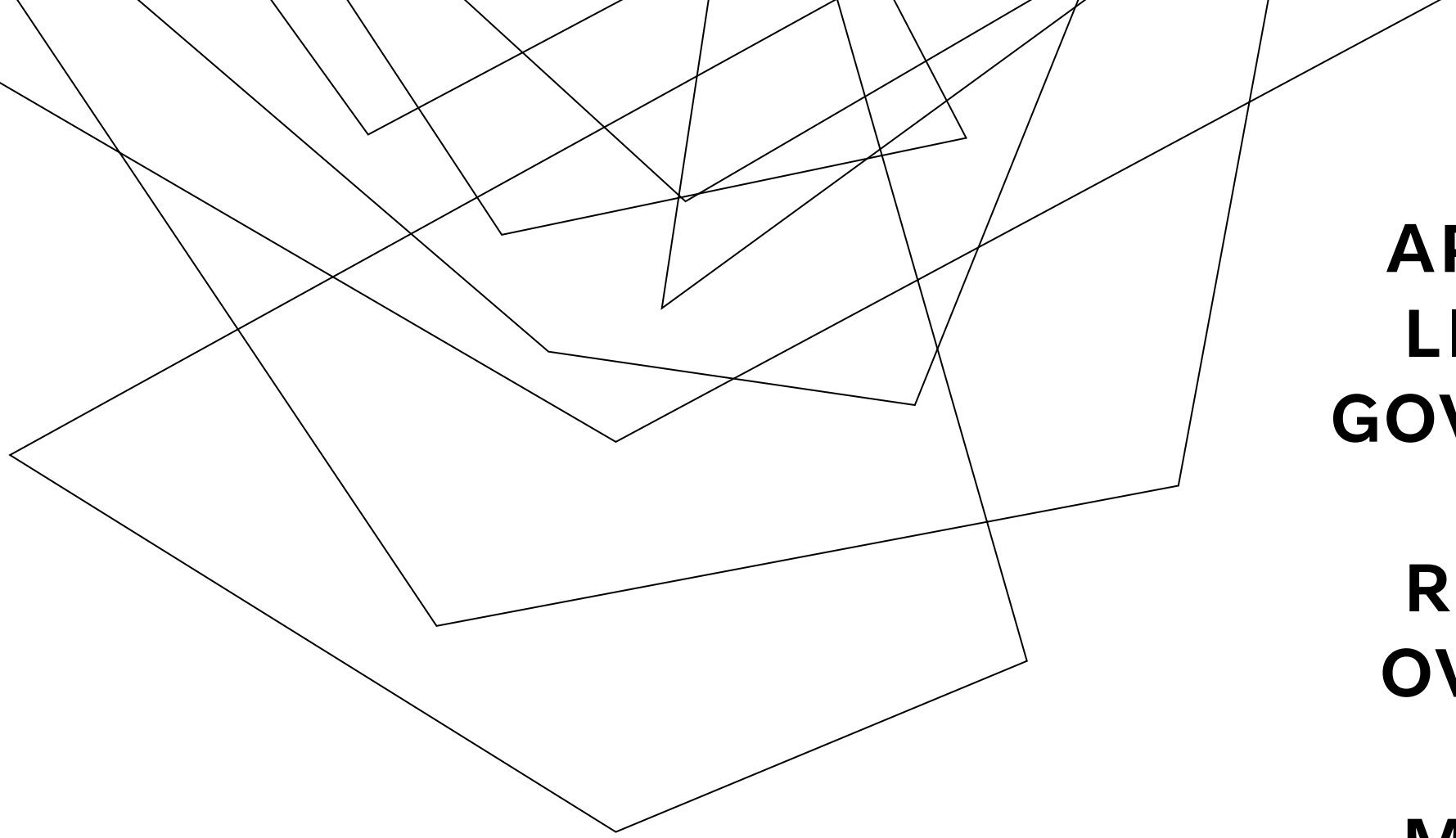


APPLIED AI LITERACY: GOVERNMENT USE, RISK, AND OVERSIGHT

MODULE 1

TEXAS DEPARTMENT OF INFORMATION RESOURCE CERTIFIED AI TRAINING
AIQ GATE - CHARLOTTE WILBORN

LEARNING OBJECTIVES

-EXPLAIN WHAT AI IS AND HOW IT WORKS

- IDENTIFY APPROPRIATE USE CASES FOR GOVERNMENT

- RECOGNIZE RISKS AND LIMITATIONS OF AI SYSTEMS

- APPLY THE 5 PILLARS OF RESPONSIBLE AI USE

- USE AI TOOLS SAFELY WITHIN AGENCY GUIDELINES

TIERS – THE CAR METAPHOR

Tier 1 – Awareness – Basics

> “I can comfortably get into the seat of the car because I understand what it is.”

Tier 2 – Comprehension – Introduction into main AI concepts

> “I can name and tell you what all the parts of the car are that I would use on a daily basis.”

Tier 3 – Application – How to effectively use AI on an everyday basis

> “I can drive the car in normal situations.”

Tier 4 – Integration – How to effectively use AI in existing workflows; AI and data risk management basics

> “I want to learn how to use a car to make my life easier, make my job easier, and understand the rules around using the car safely.”

Tier 5 – Fluency – AI Ethical Frameworks and Governance; Basics of Neural Networks, LLMs, and Machine Learning

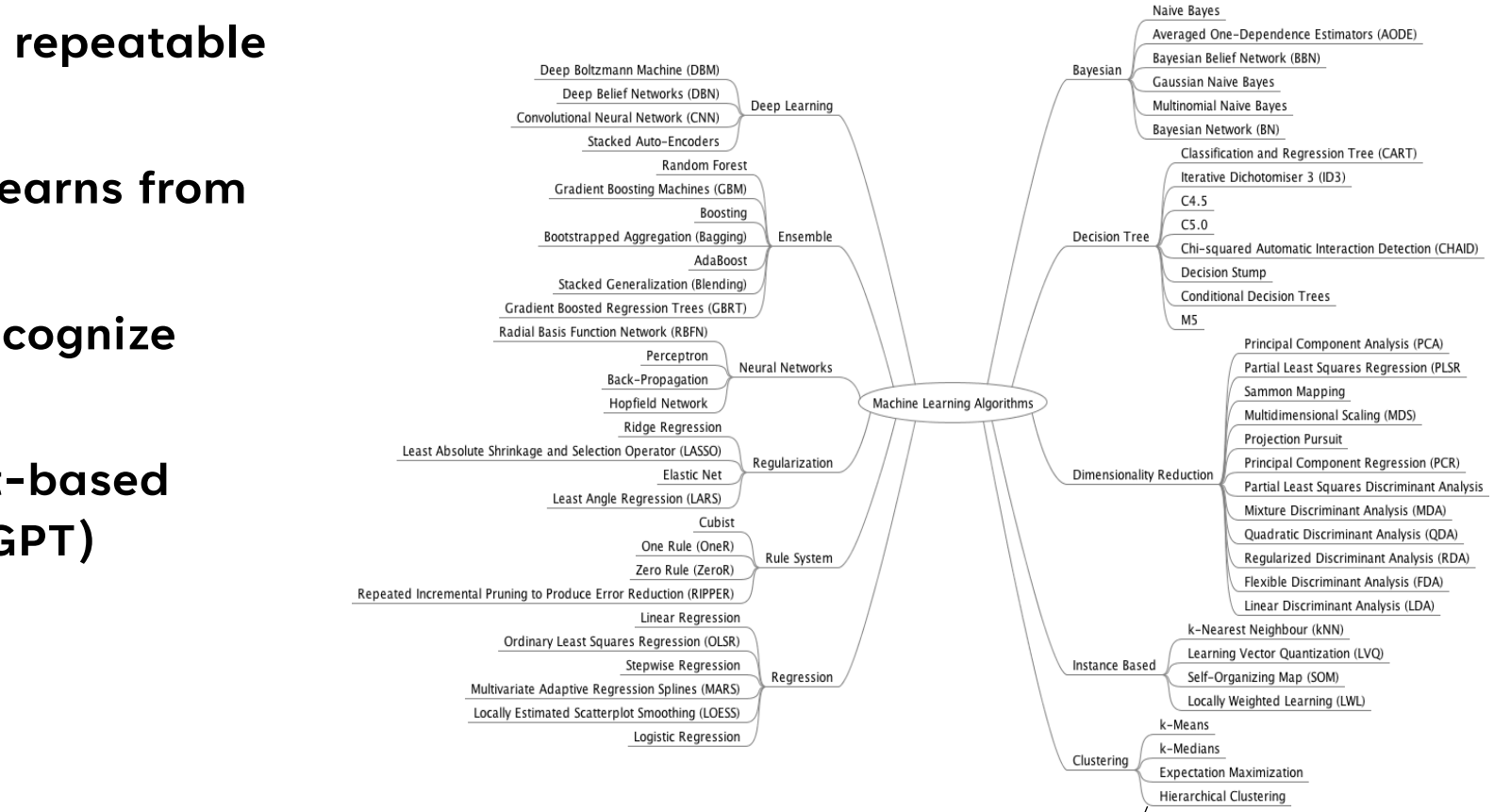
> “I can name different parts of the car that makes it go; I can understand the regulations behind the rules enacted to make it safe for everyone to drive together.”

WHAT IS AI – SIMPLE DEFINITION

- **Definition – "A machine-based system that can, for a given set of human-defined objectives, make predictions, recommendations, or decisions influencing real or virtual environments." – National Artificial Intelligence Initiative Act of 2020**
- **Artificial intelligence is a machine that learns from patterns in data and uses those patterns to make inferences with text, numbers, and other types of data.**

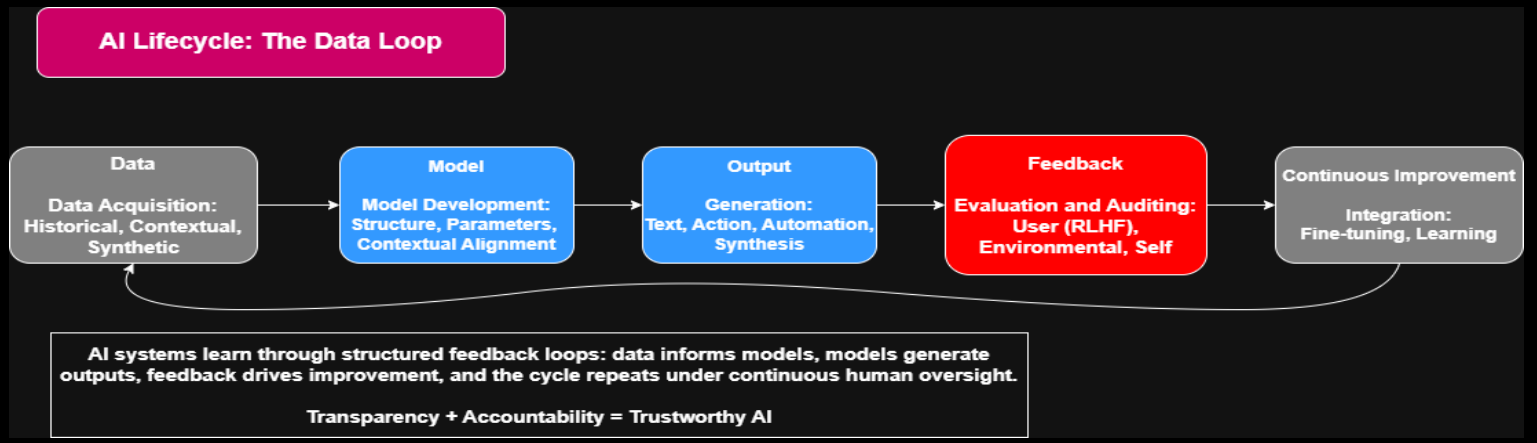
DIVISIONS OF AI – PLAIN LANGUAGE

- **Automation: Rules & repeatable tasks**
- **Machine Learning: Learns from examples**
- **Neural Networks: Recognize speech/images**
- **LLMs/Chatbots: Text-based assistants (ex. ChatGPT)**



HOW MACHINES LEARN

- INPUT > TRAINING > OUTPUT
- Input: Data entering the system
- Training: Machine finds patterns in the data
- Output: The model uses patterns to answer.
- This learning loop is called RLHF – Reinforced Learning from Human Feedback
- This is pattern recognition, not human-like reasoning.



DATA QUALITY

- GIGO
  - Garbage In = Garbage Out
- The output of any AI system is only as good as the data that it is trained on.
- Examples:
  - Biases in data = distorted results
  - Misinformation or gaps in training corpus = hallucinations
  - Unbalanced data = failed predictive analyses
- Always verify data sources and AI outputs

COMMON USE CASES AND WHY IT MATTERS

MOST AI RISK DOES NOT COME FROM ADVANCED USE. IT COMES FROM EVERYDAY USE DONE WITHOUT RISK AWARENESS.

HOW IT'S USED

- DRAFT EMAILS AND REPORTS
- SUMMARIZE DOCUMENTS
- ANALYZE SPREADSHEETS
- GENERATE CONTENT
- REFERENCE

WHAT IS HAPPENING

- EXTERNAL SYSTEM PROCESSING INTERNAL INFORMATION
- MODEL GENERATING PROBABILISTIC OUTPUTS
- DATA MAY BE RETAINED BY OUTSIDE COMPANY
- OUTPUTS MAY BE INCORRECT OR INCOMPLETE

RISK

- DATA EXPOSURE
- INCORRECT INFORMATION USED FOR DECISIONS
- MISALIGNMENT WITH POLICY
- NONCOMPIANCE
- LOSS OF TRACEABILITY

COMMON AI PLATFORMS

- CHATGPT (OPENAI) - Writing, theoretical brainstorming, summaries
- CLAUDE (ANTHROPIC) - Long document handling, structured safe responses, strong summarization
- GEMINI (GOOGLE) – Integration with Google Workspaces, image and chart analysis, fast information retrieval
- GROK (XAI) – Integrates directly with x, built for speed and innovation with direct simulation tooling

RISK AND LIMITATIONS

AUTHORIZED USAGE

AI tools should be used only according to pre-authorization and policy terms for work purposes.

- Check with IT/Cybersecurity teams before using any AI system.
- Do not use personal/consumer AI tools for government work unless pre-authorization processes have taken place.
- Always follow your organizations AI use policy.
- Unauthorized tool use may violate existing policies or the law.

When in doubt, speak to your supervisor and/or IT and cybersecurity managers.

AI LIMITATIONS

All systems have weaknesses.

1. Inaccuracy
    - May reflect outdated information
    - Cannot verify facts in real time
    - Internal incentives divergence
2. Data Quality/Training Corpus Dependent
    - Output quality reflects training and interface quality
    - Systems cannot compensate for imperfect source material
3. Lacks Judgement and Awareness
    - Systems have no contextual awareness without explicit instruction
    - Literalism: issues with understanding nuance, emotion, and ambiguity

COMMON AI FAILURES

1. Hallucinations – complex AI systems filling in information it does not actually have concrete data for and producing outputs in a confident way
    - Outputs may have false information
    - Citations may be fabricated

2. Bias – Patterns found in training data is proliferated as truth even when it is unrepresentative of the real world
    - Historical data contains bias
    - Can perpetuate discriminatory interpretations

3. Glazing (Sycophancy) – When internal incentives gravitate towards user satisfaction rather than truth
    - Systems agreeing rather than contradicting incorrect inferences
    - Adversarial analyses of reasoning or utilization of multiple platforms to mitigate

LEGAL PROHIBITIONS

LEGAL PROHIBITIONS

Texas Law prohibit using AI systems for the following categories.

Violating these prohibitions can result in legal liability.

- Social Scoring
- Biometric Identification without consent
- Any conflict of state or federal law

Comparative Analysis Table of Current AI Framework Obligations for Auditorial and Governance Compliance

Requirement	EU AI Act	NIST RMF	ISO 42001	OECD	AI Bill of Rights	TRAIGA	Council of Europe Treaty	Singapore AI Verify
Risk Assessment	Required	Required	Required	Suggested	Suggested	Required*****	Required	Suggested
Human Oversight	Required	Required	Required	Required	Required	Required*****	Required	Required
Transparency	Required	Required	Required	Required	Required (Federal Level)	Required (Government entities only)	Required	Required
Data Governance	Required	Suggested	Required	Implicit	Privacy Rights*	Implicit	Suggested	Required
Documentation	Required	Suggested	Required	Implicit	Suggested	Required**	Required	Suggested
Testing/Validation	Assessment	Suggested	Assessment	Implicit	Required	Safe Harbor***	Required	Suggested
Bias and Fairness (Mitigation & Elimination)	Required	Required	Required	Required	Required	Required	Required	Required
Incident Reporting	Required	Suggested	Required	Implicit	Not specified	Required****	Required	Not specified
Lifecycle Management	Required	Required	Required	Implicit	Suggested	Implicit	Suggested	Suggested

RISK CLASSIFICATION

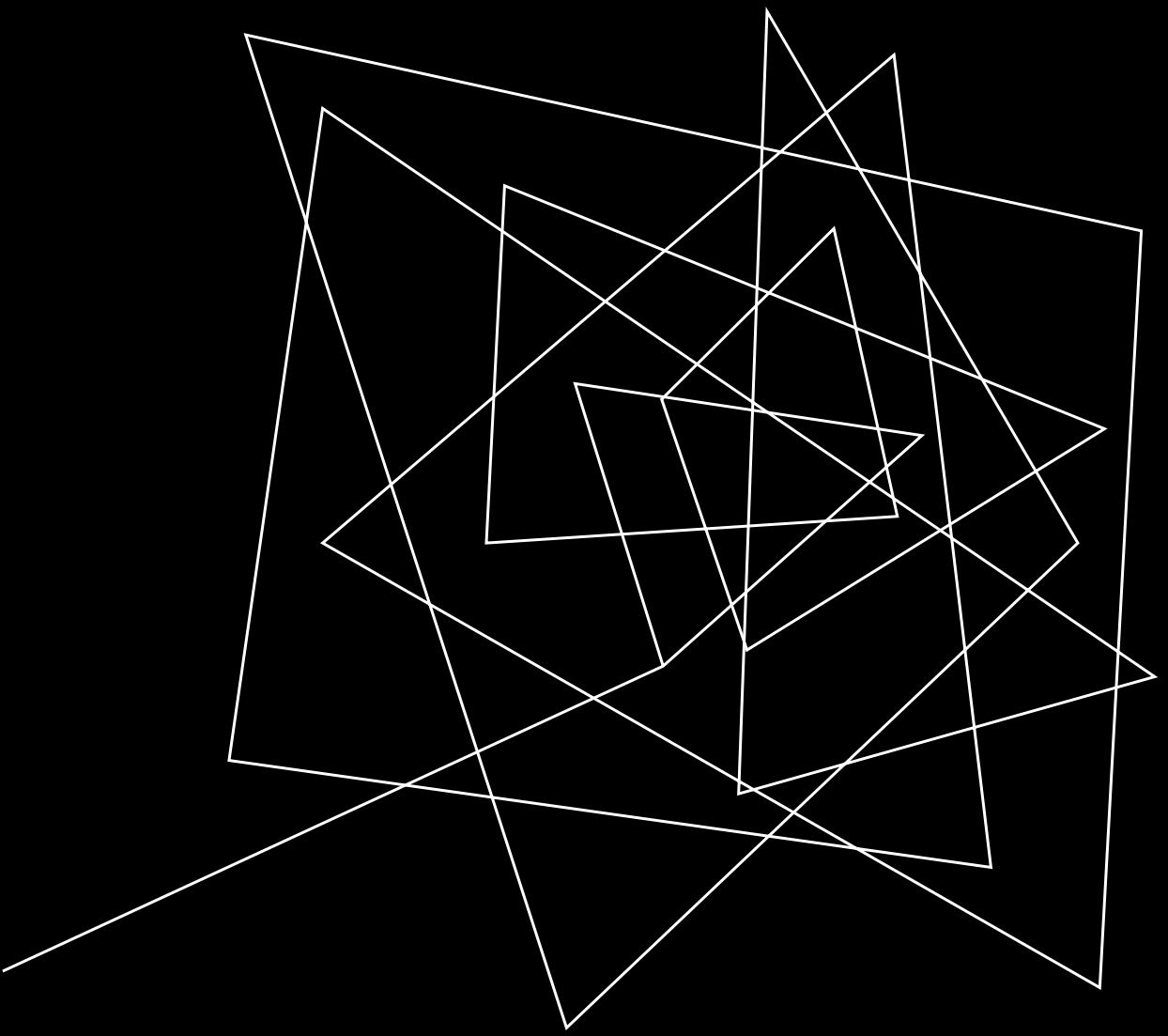
1. Low Risk
   - Summarizing publicly available documentation
   - Drafting meeting notes
   - Brainstorming for communication
2. Medium Risk
   - Analysis of citizen feedback
   - Creating public-facing content
   - Processing routine request
3. High Risk
   - Decision-making
   - Processing anything that may be considered PI (Personal Information)
   - Enforcement or compliance actions

3 GOLDEN RULES FOR AI USE

Use for drafts, ideas, research, and brainstorming – not for final products.

Protect personal and internal data.

Human-in-the-loop: Always double check results!



THE 5 PILLARS OF RESPONSIBLE AI USE

THESE PILLARS ARE NOT OPTIONAL. THEY ARE FOUNDATIONAL TO ETHICAL AI DEPLOYMENT.

- Human Oversight
- Privacy and Security
- Transparency
- Accuracy
- Accountability

HUMAN OVERSIGHT

AI outputs are reviewed and systems can be corrected.

- Never use outputs without review.
- Maintain ability to override and adjust systems.
- Monitor for negative impacts.
- Establish clear escalation procedures for failures.

Example: Approved LLM provides analyses of constituent information. Defined human staff member(s) review(s) and flag(s) interactions daily and can response to intervene directly if biases or drift of outputs occur.

PRIVACY AND SECURITY

Always protect citizen's PI when using any AI system.

- Never input identifiable/sensitive information into publicly available AI tools.
- Use only pre-authorized/secure platforms for government data.
- Follow all internal data classification procedures.

Prohibited Actions:

- Using public platforms and inputting any PI
- Uploading classified and sensitive documents into any unauthorized, public system
- Sharing constituent data without prior authorization

TRANSPARENCY

Citizens should always be informed when interacting with AI systems.

Transparency is required when:

- Chatbots or automated communication systems are used.
- AI-assisted decisions affect individual rights or benefits.
- Use of AI in consequential governmental processes.

Examples:

- “This response was generated with AI assistance and reviewed by staff.”
- “An AI system analyzed applications, and all final decisions were made by qualified personnel.”
- During interactions – Chatbot disclaimer prior to the beginning of the conversation: “You are interacting with an AI assistant. For complex issues or if you prefer to speak with a human being, please contact _____.”

ACCURACY

Verify outputs for correctness and establish monitoring practices.

Verification requirements:

- Check facts and the citations behind the facts before publication.
- Establish review workflows for AI-assisted work in appropriate categories.
- Monitor outputs for degradation of quality or drift over time.

Monitoring Processes to implement:

- Spot-checks of AI outputs.
- Track error rates and patterns.
- Update or retire systems that are deemed unreliable.
- Document verification steps.

ACCOUNTABILITY

HUMANS ARE ALWAYS RESPONSIBLE FOR ALL DECISIONS AND OUTPUTS OF AI.

GOVERNMENTS ARE RESPONSIBLE FOR THE OUTCOMES OF ANY DECISIONS MADE USING AI ASSISTANCE.

Simply Accountability:

- What is the AI tool?
- Who uses it?
- For what?
- Who reviews the output?
- Who approves the final decisions?
- Why was that decision made?

PRACTICAL APPLICATION – STARTING SAFELY

- Before you use AI:
  - Verify the tool is authorized
    - By your agency
    - For this specific use
    - To be used by you
    - This mitigates the risk of “Shadow AI” use
  - Understand what data can and cannot be used
  - Know the review requirements for your use case
  - Identify who to contact with questions

PRACTICAL APPLICATION – PROMPTING

What makes a good prompt?

- Purpose – What do you need the AI to do?
- Audience – Who is this output made for?
- Context – What is the background that the AI needs?
- Constraints – Format length, tone, requirements
- Verification – At the end, always ask “What else do you need to complete this task?”

Example
Bad: Tell me about the budget.
Good: Summarize the key changes in the FY26 budget proposal into top five key points for a public newsletter to constituents. Focus on new programs being implemented this year. Ask me questions or tell me what you need to complete this task.

PRACTICAL APPLICATION – QUESTIONS TO ASK BEFORE STARTING

1. Is this tool authorized by my agency?
2. Am I inputting any sensitive or personal information?
3. What is the risk level of this task?
4. Who needs to review the output?
5. Am I required to disclose AI use for this task?
6. Do I understand how to verify accuracy?
7. What happens if the AI output is wrong?

RESOURCES AND NEXT STEPS

Agency Resources

- AI Policy
- Data classification guidelines
- Approved AI tool list
- Training and support contacts

DIR Resources

- Texas AI Code of Ethics
- TRAIGA Framework
- Certification Standards
- Advisory board guidance

OVERVIEW

AI is a powerful tool for efficiency...when used responsibly.

- AI assists; humans decide and act.
- Use only authorized tools for authorized uses.
- Protect constituent information.
- Verify all outputs.
- Follow the 5 Pillars:
  - Oversight
  - Privacy
  - Transparency
  - Accuracy
  - Accountability

Q & A

THANK YOU

Charlotte Wilborn
Charlotte@AIQGate.com
Document Title: APPLIED AI LITERACY: GOVERNMENT USE, RISK, AND OVERSIGHT - MODULE 1
Version 1.0

Revision Date	Revision Summary
03.18.2026	Created original PPT/PDF.

AI Disclosure Statement:
This document was generated through human-AI collaboration with the use of ChatGPT/Claude/Grok. All content has been reviewed for alignment with NIST RMF and ISO 42001 standards in compliance with current AI data governance as of 03/18/2026.