Policy Approaches and Risk Management for Artificial Intelligence

Presentation to the Courts, Corrections, and Justice Interim Committee

Jeff Lopez
Director
NM Office of Broadband Access and Expansion
August 26, 2026

CONNECT new mexico
Office of Broadband Access & Expansion

I. Agenda

I.
II.
III.
IV.
V.
VI.

I. **Agenda -** Why I'm Here

II. **Taxonomy** for Artificial Intelligence

III. **Federal Action** on AI

- Congress and Executive Orders
- NIST AI Risk Management Framework
- AI in Critical Infrastructure

IV. **Risk Management** for New Mexico Infrastructure

V. **Resources** for Policymakers

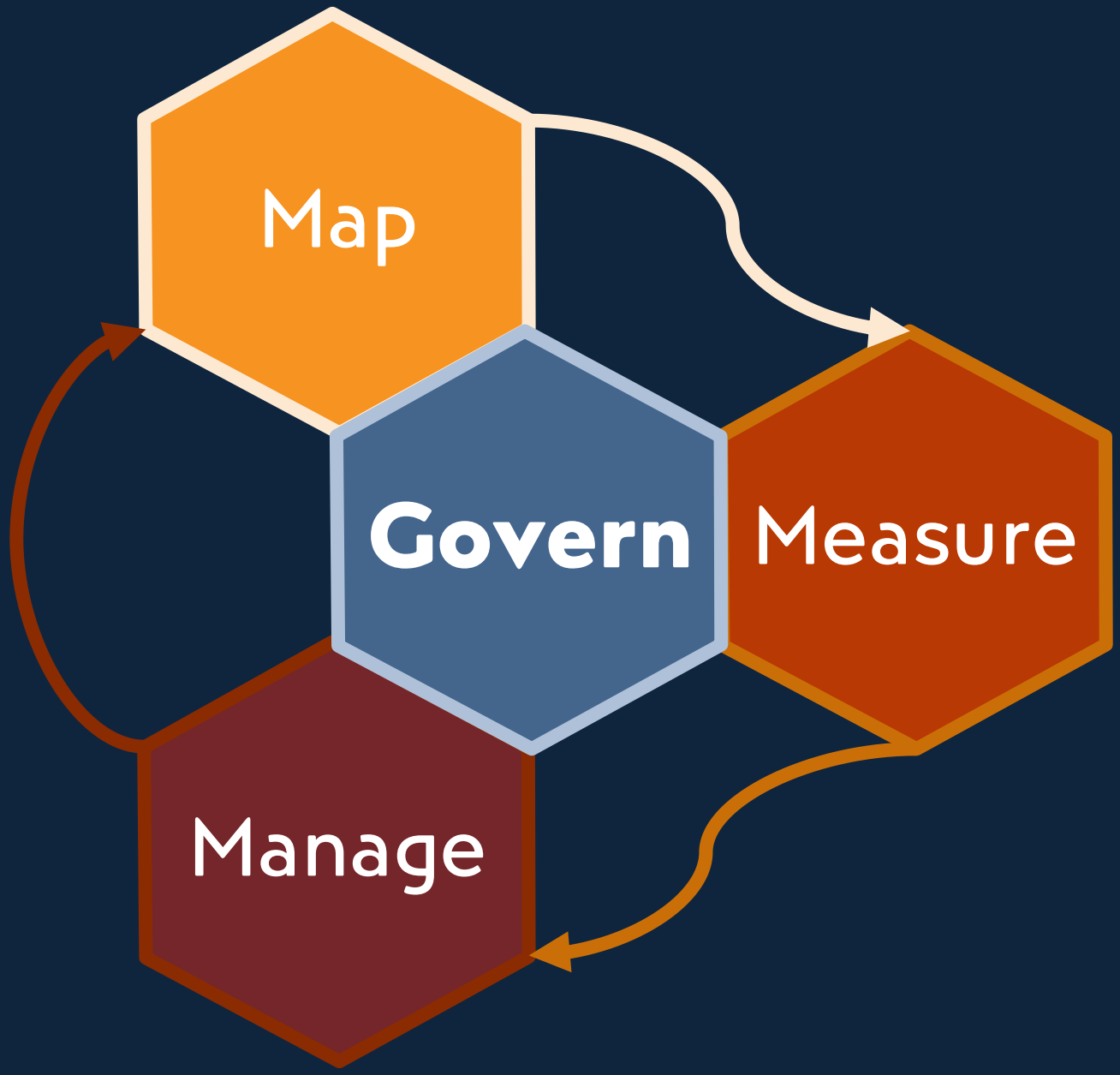
VI. **Recommendation:** Improve the State's capacity to Govern, Map, Measure, and Manage AI

I.
II.
III.
IV.
V.
VI.

I. Agenda
Why I'm Here

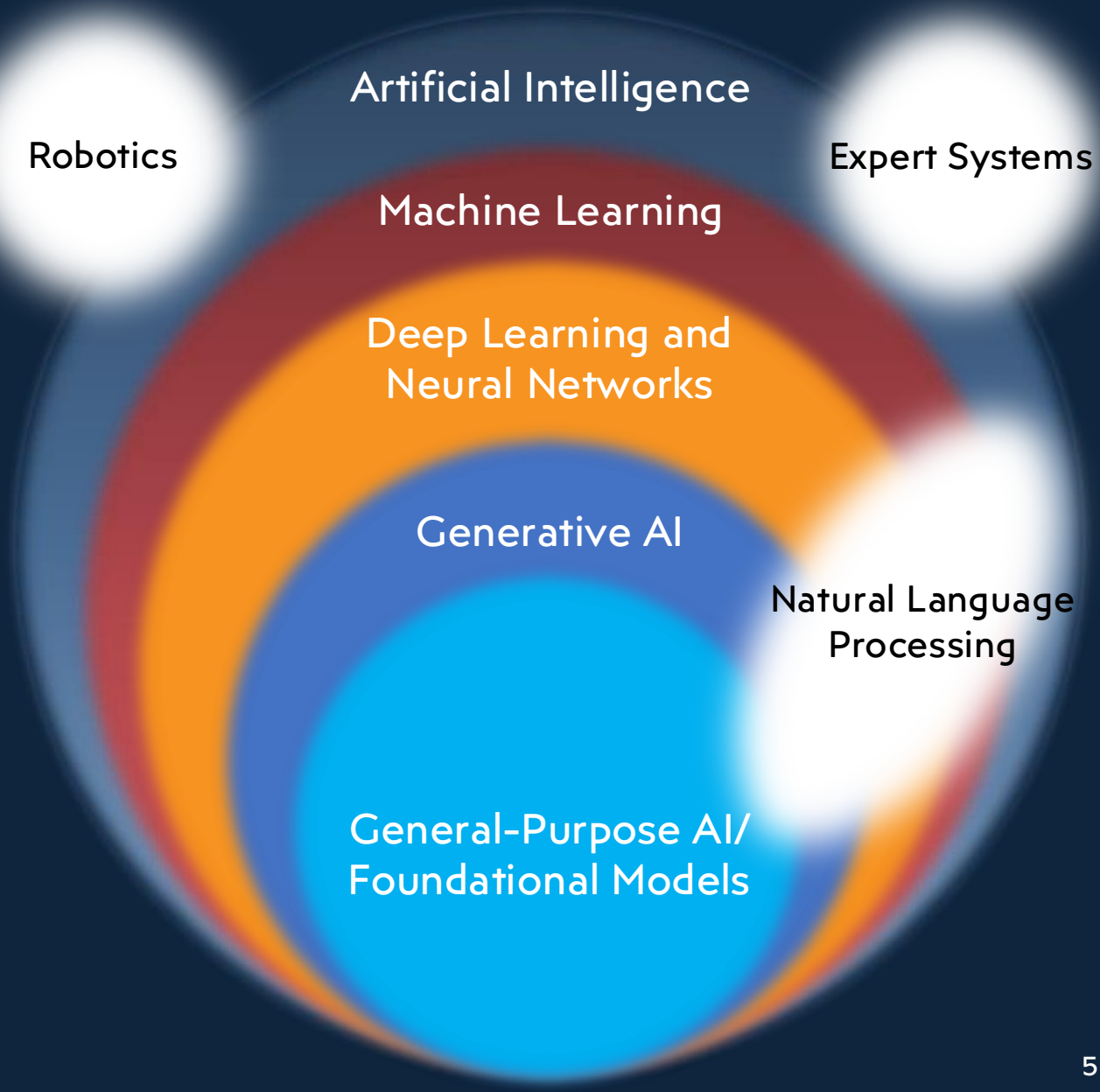
- OBAE Mission
  - Broadband: Last mile, middle mile, long haul fiber
  - Education and Consumer Protection: Digital Literacy
  - Federal Compliance: CIPA/COPPA under E-Rate
  - Tribal Sovereignty and Collaboration
- OBAE Resources
  - Middle Mile Map
  - Permitting and Right of Way
- Risk to BEAD – AI Executive Order
- 14 Years Staff in the United States Senate

II. Taxonomy
for AI



Source: AI Risk Management Framework, National Institute of Standards and Technology (NIST), January 2023

II. Taxonomy
for AI



Source: Laurie Harris, "Artificial Intelligence (AI) Taxonomy". Congressional Research Service, Library of Congress, April 2025

II. Taxonomy for AI

Artificial Intelligence [System]:

FEDERAL STANDARDS

an engineered or machine-based system that can, for a given set of objectives, generate outputs such as predictions, recommendations, or decisions influencing real or virtual environments. AI systems are designed to operate with varying levels of autonomy.

(NIST AI RMF, adapted from OECD Recommendation)

STATE LAW

an engineered or machine-based system that varies in its level of autonomy and that can, for explicit and implicit objectives, infer from the input it receives how to generate outputs that can influence physical or virtual environments.

(HB 28 – 2026) compare to NMSA §1-19-26 and NMSA §61-3-3

FEDERAL LAW

a machine-based system that can, for a given set of human-defined objectives, make predictions, recommendations or decisions influencing real or virtual environments. Artificial intelligence systems use machine and human-based inputs to- (A) perceive real and virtual environments; (B) abstract such perceptions into models through analysis in an automated manner; and (C) use model inference to formulate options for information or action.

(P.L. 116-283)

I.
II.
III.
IV.
V.
VI.

III. Federal Action on AI

A. Congress
B. Executive Orders
C. NIST AI Risk Management Framework
D. AI in Critical Infrastructure

III. Federal Action

A. Congress

- No federal legislation establishing regulations for the development or use of AI or prohibitions on AI – NO PREEMPTION… yet
- Congress debating between regulating AI (safety, averting risk, security) and accelerating innovation
- In the absence of legislation, U.S. instead focused on 1) executive action through the White House or federal agencies, 2) whether federal agencies need additional authorities; and 3) voluntary commitments from industry

Source: Harris, Laurie, "Regulating Artificial Intelligence: U.S. and International Approaches and Considerations for Congress". Congressional Research Service, Library of Congress, June 2025

III. Federal Action

B. Executive Action

EO 14365 (December 2025)

- Evaluation of State AI laws
- Targeted Colorado AI Act which was then repealed and replaced by the Automated Decision-Making Technology Act (ADMTA) in June 2026
- June 2026 FTC Policy Statement "address how State laws requiring alterations to the accurate outputs of AI models can conflict with the requirements of the FTC Act"
- NTIA forthcoming guidance on BEAD non-deployment funding ($280 million to NM OBAE)

EO 14409 (June 2026)

- Security of frontier models

III. Federal Action

C. NIST AI Risk Management Framework

Equip organizations and individuals who play an active role in AI system lifecycle:

"offer a resource to the organizations designing, developing, deploying, or using AI systems to help manage the many risks of AI and promote trustworthy and responsible development and use of AI systems"

RMF intent:

- flexible
- voluntary
- rights-preserving
- non-sector-specific
- use-case agnostic

Source: Tabassi, Elham. Artificial Intelligence Risk Management Framework (AI RMF 1.0). NIST AI 100-1. Gaithersburg, MD: National Institute of Standards and Technology, 2023.

III. Federal Action

C. NIST AI Risk Management Framework

Framing Risk

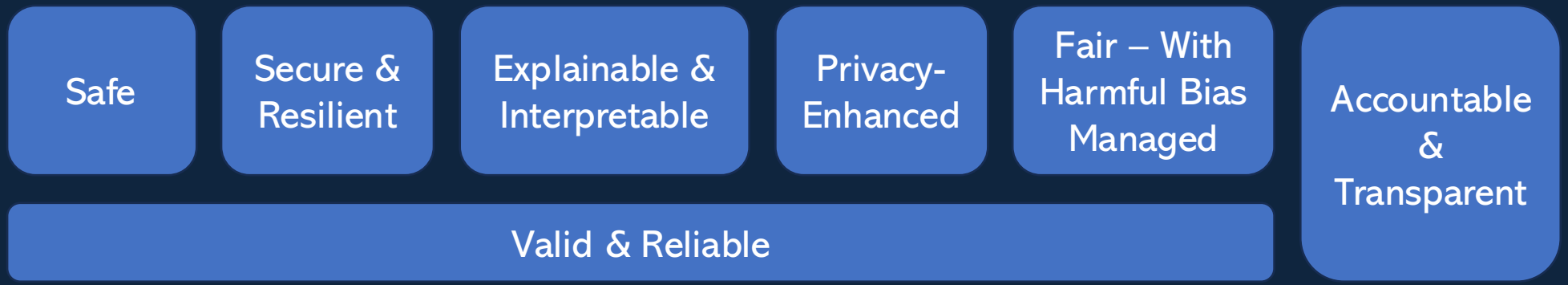
Harm to People	Harm to an Organization	Harm to an Ecosystem
• **Individual**: Harm to a person's civil liberties, rights, physical, or psychological safety, or economic opportunity. • **Group/Community**: Harm to a group such as discrimination against a population sub-group. • **Societal**: Harm to democratic participation or educational access.	• Harm to an organization's **business** operations. • Harm to an organization from **security** breaches or monetary loss. • Harm to organization's **reputation**.	• Harm to interconnected and interdependent elements and resources. • Harm to the global **financial system**, supply chain, or interrelated systems. • Harm to **natural resources**, the **environment**, and planet.

Source: Tabassi, Elham. Artificial Intelligence Risk Management Framework (AI RMF 1.0). NIST AI 100-1. Gaithersburg, MD: National Institute of Standards and Technology, 2023.

III. Federal Action

C. NIST AI Risk Management Framework

AI Risks and Trustworthiness



Source: Tabassi, Elham. Artificial Intelligence Risk Management Framework (AI RMF 1.0). NIST AI 100-1. Gaithersburg, MD: National Institute of Standards and Technology, 2023.

III. Federal Action

C. NIST AI Risk Management Framework

AI System Lifecycle

Key Dimensions	Application Context	Data & Input	AI Model	AI Model	Task & Output	Application Context	People & Planet
Lifecycle	Plan and Design	Collect and Process Data	Build and Use Model	Verify and Validate	Deploy and Use	Operate and Monitor	Use or Impacted by
Testing, Evaluation, Verification, Validation	Audit & impact	Internal & external validation	Model testing	Model testing	Integration & compliance	Audit & impact	Audit & impact

Source: Tabassi, Elham. Artificial Intelligence Risk Management Framework (AI RMF 1.0). NIST AI 100-1. Gaithersburg, MD: National Institute of Standards and Technology, 2023.

IV. AI in Critical Infrastructure

IV. AI in Critical Infrastructure

NIST AI RMF Profile on Trustworthy AI in Critical Infrastructure (Discussion Draft) intentionally deconflicted from cybersecurity

- Chemical
- Commercial Facilities
- Communications
- Critical Manufacturing
- Dams
- Defense Industrial Base
- Emergency Services
- Energy
- Financial Services
- Food & Agriculture
- Transportation Systems
- Information Technology
- Healthcare & Public Health
- Nuclear Reactors/Materials/Waste
- Government Services & Facilities
- Water & Wastewater Systems

Source: NIST AI RMF Profile on Trustworthy AI in Critical Infrastructure, Community of Interest Discussion Draft, August 3, 2026

IV. AI in Critical Infrastructure

	Description	Risk Management
Incident 1 Dutch childcare benefits scandal (Toeslagenaffaire) (Government Services)	Machine learning module used by the Dutch tax authority wrongly flagged non-Dutch families for benefit termination	3) Define risks 8) Incident response 9) Provide AI-aware training
Incident 2 Detroit facial recognition wrongful arrest (Emergency Services)	Police department relied on facial-recognition match (9th best)	2) Define robustness 3) Define risks 9) Provide training
Incident 3 Air Canada chatbot hallucination (Transportation)	Generative AI customer-service chatbot fabricated bereavement-fare policy that contradicted with actual	1) Establish requirements 2) Define robustness 12) Validate AI-generated logic

Source: NIST AI RMF Profile on Trustworthy AI in Critical Infrastructure, Community of Interest Discussion Draft, August 3, 2026

IV. AI in Critical Infrastructure

actionable risk management activities

Practice 1: Establish requirements for success

Practice 2: Define AI Robustness, Resilience, and Quality of Service expectations

Practice 3: Define risks, policies, and oversight for automated AI and agentic behavior

Practice 4: Define procedures for emergency avoidance override, recovery, and situation awareness

Practice 5: Implement identity and access management for AI agents, systems, and tools

Practice 6: Integrate visibility of the external supply chain of AI into vendor and 3rd party risk management

Practice 7: Manage internal AI supply chain and data provenance

Practice 8: Incorporate AI-aware incident analysis and response procedures

Practice 9: Provide calibrated, needs-based risk management training

Practice 10: Implement multi-tiered AI system logging and audit capabilities

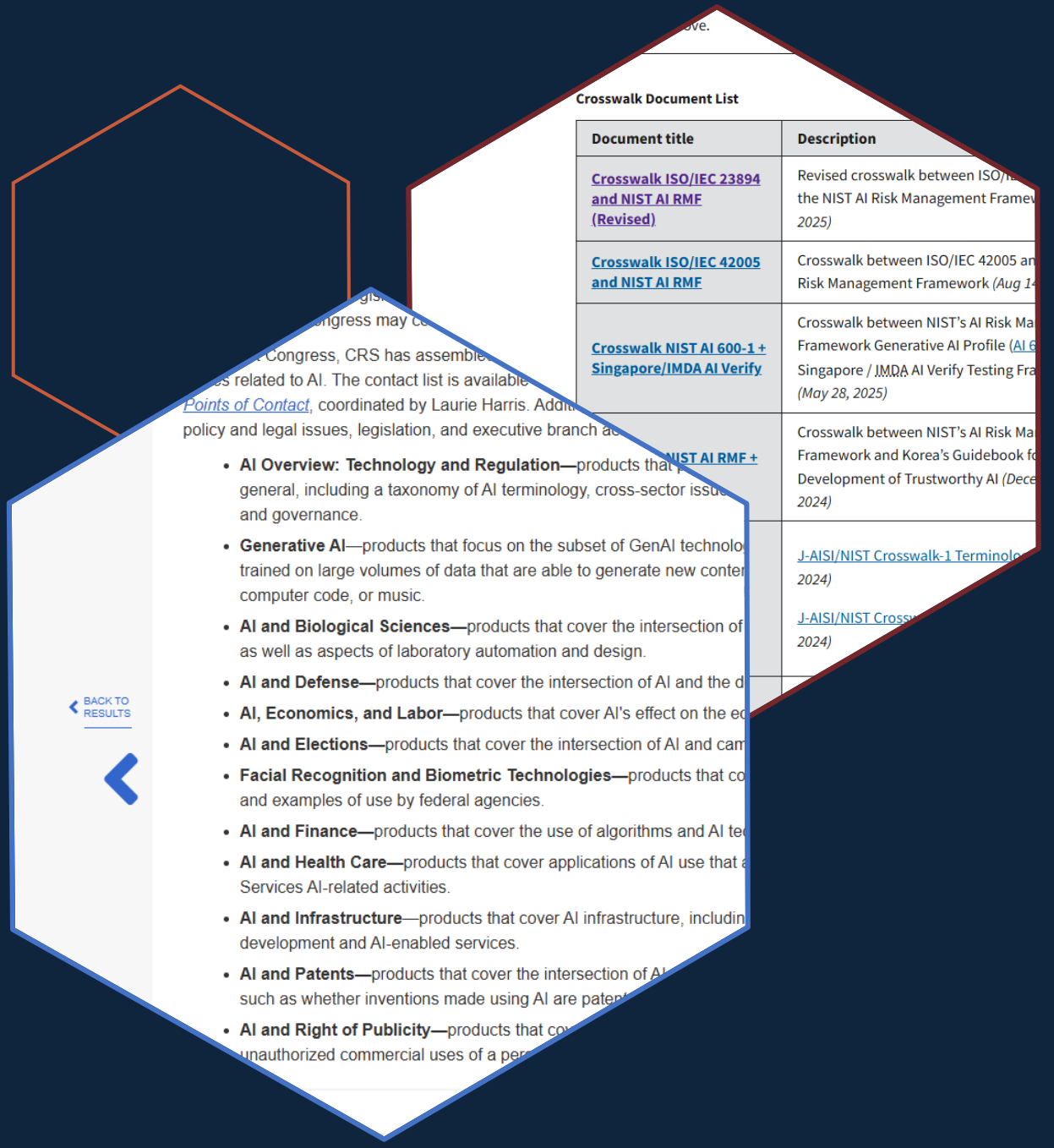
Practice 11: Maintain AI-aware mission continuity and disaster recovery planning

Practice 12: Validate AI-Generated Operational Logic and Artifacts

Source: NIST AI RMF Profile on Trustworthy AI in Critical Infrastructure, Community of Interest Discussion Draft, August 3, 2026

V. Resources

- NIST AI Risk Management Framework, 2023
- NIST AI Resource Center (AIRC)
- NIST AI RMF Crosswalk
- AI RMF Profile on Trustworthy AI in Critical Infrastructure Concept Note and Discussion Draft
- Congressional Research Service Products: Artificial Intelligence
- NCSL's Artificial Intelligence Database



V. Resources

NM AI Consortium

Sandia National Laboratories · The University of New Mexico · Los Alamos National Laboratory · CNM Central New Mexico Community College · NM State University · New Mexico Consortium · New Mexico Tech

VI. Recommendation

The State of New Mexico must improve its capacity to **govern** AI: **map**, **measure**, and **manage**.

Thank you

Jeff Lopez

jeff.lopez@connect.nm.gov

505-618-0340