Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence

A summary of Executive Order 14110: Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence, signed on October 30, 2023 by President Biden:

Key Points

1. Purpose and Vision

- Establishes the first comprehensive U.S. government framework for AI development and deployment.
- Aims to balance innovation with safety, equity, civil rights, and national security.

---

2. Key Directives Across Sectors

🛡️ **AI Safety & Security**

- **Red Teaming & Testing:** Developers of powerful AI systems (especially foundation models) must conduct rigorous safety testing (including for biological, chemical, cyber, and other risks) before public release.
- Reporting Requirements: Developers must notify the federal government if models exceed specified computational thresholds.
- National AI Research Resource (NAIRR): Reinforced to promote shared access to AI compute infrastructure for researchers and startups.

📜 **Privacy Protection**

- Encourages development of privacy-enhancing technologies (PETs) like federated learning.
- Pushes for federal data privacy legislation and evaluation of how AI may erode privacy.

⚖️ **Equity, Civil Rights & Justice**

- Directs agencies (like DOJ, HUD, and EEOC) to ensure AI does not perpetuate discrimination in housing, employment, or criminal justice.
- Promotes algorithmic fairness and civil rights audits for federal AI use.

💼 **Labor & Workforce Impact**

- Calls for a report on AI's labor market effects and strategies to mitigate job displacement.
- Promotes AI upskilling and reskilling programs via the Department of Labor.

🔓 **Transparency & Accountability**

- Development of clear AI watermarking and content provenance standards to combat deepfakes and misinformation.
- Mandates disclosure when AI is used in federal decision-making that affects individuals.

Use of AI in Government

- Agencies must inventory current and planned AI systems.
- Promotes responsible federal procurement and risk management for government AI tools.

---

3. Cross-Agency Collaboration

- Establishes an AI Council led by the White House to coordinate AI policy implementation.
- **Requires NIST (National Institute of Standards and Technology) to set technical standards for AI safety and trustworthiness.**

Area	Significance
Public Safety	Strong guardrails for powerful models to prevent misuse.
Civil Rights	First AI executive order to **directly tackle bias and fairness.**
Global Leadership	Sets a precedent for **democratic governance of AI**, contrasting China's approach.
Industry Impact	Impacts how major AI companies (like OpenAI, Google, Microsoft) test and release models.

In Summary

Executive Order 14110 is the U.S. government's most sweeping action on AI to date. It:

- Demands responsible AI innovation that protects rights and safety.

- Requires federal agencies and AI companies to adopt risk mitigation, testing, and transparency measures.
- Lays the foundation for future legislation, governance, and international coordination.