Rachakonda Hrithik Sagar
2023900021

RSAI - Activity 3

Executive Order on Safe, Secure, and Trustworthy Artificial Intelligence
What to do?

1. Please go through the FACTSHEET
2. Submit the following.

- At least 3 technical issues that are highlighted in the Order.
- At least 3 ideas that you think you can take up as a course project

Answers:

1. At least 3 technical issues that are highlighted in the Order.

Ans)
Technical issues that are addressed in the order are:

- Developing a standardized framework for sharing safety test results of powerful AI systems to make them safe, secure, and trustworthy.
- Protect against fraud and deception by detecting AI-generated content and authenticating official content.
- Establishing an advanced cybersecurity program to develop AI tools for finding and fixing software vulnerabilities.
- There is a national security memorandum on AI to address technical challenges and navigate complexities related to AI integration into military and intelligence operations.

Some of the direct orders are:

1. New Standards for AI Safety and Security
2. Protecting Americans' Privacy
3. Advancing Equity and Civil Rights
4. Standing Up for Consumers, Patients, and Students
5. Supporting Workers
6. Promoting Innovation and Competition
7. Advancing American Leadership Abroad
8. Ensuring Responsible and Effective Government Use of AI

2. At least 3 ideas that you think you can take up as a course project.

Ans)

1. AI safety assessment program
2. A proposed solution is to implement a watermarking system for content generated through AI. For instance, when content is copied directly from AI-generated sources like ChatGPT, Copilot, or Google's Bard, this content should be watermarked in a way that is impossible to remove. This will help readers identify the source of the content they are reading.
3. Checking if private data has been used without consent.