Cognitive Artificial Intelligence

Background and Description

- As artificial intelligence tools become more and more utilized throughout government and commercial industries, it is important to understand the capabilities, limitations, risks, and ethical issues that may affect future test and evaluation of cognitive AI tools.
- Currently, the testing community has research gaps in these areas. Cognitive Artificial Intelligence efforts aim at producing a general artificial intelligence system that can perform tasks that are normally far too complex for the human brain to process.
- Such use cases include cleaning and processing large amounts of data, making predictions and inference on large data sets and developing autonomous, or near-autonomous systems that can assist in human decision-making.

Approach

- Document the challenges of Cognitive AI-systems, the goals of developing such technology and potential gaps in the technology
- Develop processes and procedures for classifying and cataloguing AI-enables systems and tools. Document the requirements needed to adequately evaluate the operational and ethical performance of AI-enabled systems
- Team with other stakeholders (e.g. GTRI, Virginia Tech, TETRA Analysts) to establish research, investigate policies, metrics and standards
- Develop the testing requirements needed to evaluate the operational, ethical, and security performance of AI-enabled systems-informing the artificial intelligence learning red team to assess testing and evaluation limitations and develop improvements
- Develop testing metrics (measures of performance and measures of effectiveness) for assessing the performance of emerging AI-technologies, with particular emphasis on security, ethics, and operational performance of these systems
- Develop a risk-based framework specifically for the test, evaluation, and system safety of AI-enabled systems
- Develop the requirements and processes for the AI learning red team

Objectives

- Provide recommendations on areas that T&E Community should focus with respect to training data for AI algorithms; standards and test metrics for algorithm performance, effectiveness, and suitability.
- Document the challenges of incorporating Cog AI solutions into testing
- Develop methods for automated training and testing of AI/ML algorithms including neural networks and large language models.
- Develop strategy, testing requirements and evaluation processes for the AI learning Red Team.

Risks and FY24 Considerations

Risks	FY24 Considerations
N/A	Identify specific technologies in development that test methodologies could apply to
	Identify specific T&E testing policies that need to be modernized.