CapitalOne-Illinois Center for Generative AI Safety, Knowledge Systems, and Cybersecurity (ASKS)
Call for Proposals 2025-2026

Abstracts Due: May 9, 2025
Full Proposals Due: **July 6, 2025**

1. INTRODUCTION

Generative Artificial Intelligence Models (GAIMs) have emerged as transformative tools, driving advancements across diverse domains. However, their widespread adoption raises critical concerns regarding trustworthiness across dimensions such as truthfulness, safety, cybersecurity, fairness, robustness, and privacy. These models have demonstrated remarkable performance on knowledge reasoning tasks, owing to their implicit knowledge derived from extensive pretraining data. However, their inherent knowledge bases often suffer from disorganization and illusion, bias towards common entities, and rapid obsolescence. Consequently, GAIMs frequently make up untruthful information, exhibit resistance to updating outdated knowledge, or struggle with generalizing across multiple languages. The CapitalOne-Illinois Center for Generative AI Safety, Knowledge Systems, and Cybersecurity (ASKS) is a collaboration between CapitalOne and University of Illinois Urbana-Champaign, aims to advance GAIMs' up-to-date knowledge, safety, truthfulness, trustworthiness across multiple dimensions and model types, and paving the way for safer and more responsible integration of GAIMs into critical applications including cybersecurity and situation understanding.

2. CFP 2025-2026 TOPICS

The ASKS Center is calling for proposals for the second funding round, 2025-2026 academic year. In this phase, the center will support 3-5 sponsored projects. Each funded project will support a PhD research assistant and 2-4 weeks of summer salary for principal investigators (PIs). Each selected project will then engage with research scientists from CapitalOne to collaborate and jointly advise PhD students.

Topics of interest would include, but are not limited to, those below. Please feel free to bring your unique viewpoint and expertise to these topics:

<u>Large Language Models (LLMs) and Vision Language Models (VLMs) Safety:</u>

- LLM Reasoning, System 2 Thinking
- LLM agents
- Creative Intelligence
- Guardrail models and agents
- Synthetic Data Generation
- Jailbreaking, prompt injection, and their defenses
- Inference attacks, extraction attacks, and their defenses
- Hallucination Mitigation, LLM and VLM factuality
- Multimodal knowledge representation
- Knowledge localization, updating and editing

- Debiasing and Unlearning
- Theme-based and structure-enhanced RAG (retrieval augmented generation)
- Privacy Preservation
- Human-Model Alignment

Knowledge Systems:

- Open-domain Never-Ending Knowledge Extraction, Discovery and Acquisition
- Knowledge base construction and operation
- Anomaly Event Detection
- Situation Understanding, Forecasting and Reporting
- LLM-enhanced information extraction and knowledge graph construction

CyberSecurity:

- Multi-dimensional anomaly detection
- LLM for Explanation
- Time Series Data Mining
- Temporal Spatial Aware Foundation Models
- AI for cybersecurity
- Privacy-preserving data analytics

3. PROPOSAL GUIDELINES

- Eligibility: Full-time tenure-track, research-track and teaching faculty members at Illinois are eligible to submit proposals as PIs.
- Submissions should not reference either CapitalOne, nor speculate about how the research might be applied to current or future CapitalOne products, services, business models or needs. Proposals should focus on science.
- Stage 1 abstract submissions are due **May 9, 2025**. Interested CapitalOne faculty submit a **1-page maximum overview** (excluding references) of a potential full proposal. The purpose of these abstracts is for CapitalOne to review and provide feedback on the proposal: would CapitalOne be interested in collaborating with this researcher, could the proposal include new use cases for the science, and does the project align with industry goals. Feedback will help guide the faculty member towards submitting a more relevant and impactful proposal. Abstracts are not a prerequisite for submitting proposals. A PDF of the 1-page abstract should be submitted to: Link **on or before May 9, 2025, at midnight CDT.**
- An ASKS abstract feedback session will be held between **May 12 - June 16, 2025**. The CapitalOne Science review team will give feedback on whether a full proposal is encouraged for each abstract submission. It is hoped that this exchange will serve as a matchmaking exercise, enabling the development of well-focused proposals that are aligned with the interests of the PI and CapitalOne.
- Stage 2 full proposal submissions are due **July 6, 2025**. PIs who did not submit abstracts are still eligible to submit full proposals. The proposal should not exceed three pages, with unlimited references. PIs are encouraged to seek collaborations with research scientists at CapitalOne to prepare for proposals.

- Full Proposal Format: The proposal format is single-spaced, 11-point font or larger, with no less than 0.5-inch page margins. The proposal should include the following content:
    - Full names and email addresses of all PIs involved
    - Project description (3 pages max), including the focus area of the proposal (per Call for Proposal process), title, PI(s), an executive summary, technical description of the project, expected deliverables/outcomes, milestones, and what plans exist for open sourcing data or results
    - List all university background IP (unlimited)
    - References (unlimited)
    - Requested budget (1 page max), use format shown in Section 7
    - Biographies of the PIs (up to 3 pages per PI in NSF Format)
- Selection criteria: Proposals will be evaluated by a collaborative advisory board composed of ASKS Leadership Team (excluding board members who submitted proposals) and CapitalOne scientists. Successful projects will be evaluated on their technical merits and innovations, topic relevance, potential to advance research in focus areas, promise and progress in the quality of publications, student mentoring, potential technology transfer activities, and broader impacts.
- Project period of performance: September 1, 2025–August 31, 2026.

4. Important Dates

- April 18, 2025: CFP Topics Announced
- May 9, 2025: Abstract Submission Deadline
- June 18, 2025: Information Session
- May 9 – June 20, 2025: Abstract feedback sessions with CapitalOne scientists and UIUC Faculty
- July 6, 2025: Full Proposal Submission Due
- August 6, 2025: Full Proposal Acceptance Notification
- September 2025 (On Campus ASKS Center Event)

5. Submission and Contact Information

PDFs of the submission documents should be uploaded to HERE. For questions about the proposal submission process, please contact [asks-management@lists.cs.illinois.edu]. For questions about the ASKS Center, please contact the center director Prof. Heng Ji [hengji@illinois.edu] or the leadership team: [asks-leadership@lists.cs.illinois.edu].

6. ASKS Leadership Team

- Director: Heng Ji (Illinois)
- Associate Director: Gang Wang (Illinois)
- Center Liaison: Prem Natarajan (CapitalOne)
- Program Manager: Katie Clark (CapitalOne)
- Center Alliance Manager: Kelly McKinley (Illinois)

- Advisory board members: Jiawei Han (Illinois), Bo Li (Illinois), Milind Naphade (CapitalOne), Ling Ren (Illinois), Sambit Sahu (CapitalOne), Gokhan Tur (Illinois)

7. BUDGET FORMAT

Work with your department's business office to complete a budget table in the format shown below. The categories and text in the "basis of estimate" column are provided as examples; please update to reflect actual expenses and project needs.

Per the Collaboration Agreement, no F&A costs are to be assessed on Gift-Funded Research Projects. If, through the review process, the project is deemed to be a Sponsored Research Project, budgets will be renegotiated.

Item	**Amount**	**Basis of Estimate**
PI Summer Salary	$XX	2 weeks of summer salary, including fringe benefits
GRA Salary Support	$XX	X-months GRA at Y% effort, including fringe
Other Direct Costs	$XX	List items. E.g., hard drives, high-speed cluster access, publication fees, software costs, travel
Total	$XX	