ILLINOIS

Office of the Vice Chancellor for Research & Innovation

National Center for Supercomputing Applications
1205 W. Clark St.
Urbana, IL, 61801

November 1, 2025

Dear Search Committee,

I am writing to explain how my research strengthens AI/ML supercomputing infrastructure to deliver reliability, security, and correctness in $\$100M$-scale supercomputers and research computing clusters operations.

My background as a Principal Investigator at the National Center for Supercomputing Applications (NCSA), coupled with my deep expertise in curating longitudinal data of system-wide outages and security incidents, is critical for enabling AI training. My operational research experience with the Blue Waters/DeltaAI supercomputer and cutting-edge Quantum-resistant cryptography will provide real-world data to guide the minimization of cyberinsurance risk. More importantly, I will bring case studies of decisions in critical infrastructure, e.g., optimizing total cost of ownership in GPU clusters, which is a trillion-dollar business for hyperscalers.

In summary, my research agenda *Resiliency and Security of AI supercomputers* is at the nexus of analytics applications with critical business impact. I will contribute to the department as follows:

A. Research Excellence at the Intersection of AI, Bayesian Analytics, and Supercomputers

I have secured over $1.5 million in grants from the federal government and industry. As PI and Co-PI, I have published over 20 peer-reviewed papers in top venues such as the IEEE Quantum Computing and Engineering (QCE), USENIX Security, Best Paper Award at IFIP Dependable Systems and Networks, Art of HPC showcased at the International Conference for High Performance Computing, Networking, Storage and Analysis (Supercomputing).

(1) Active research portfolio $> \$1.5M$ of already granted awards on advanced cyberinfrastructure security with operational experiences of Generative AI agents, demonstrated through 04 National Science Foundation awards as PI and publications in top CS/ECE conferences.

(2) Real-world knowledge of statistics in business domains such as supercomputing, health analytics, and cybersecurity, demonstrated through curation of more than one petabyte of supercomputing performance data. This will bring real-world case studies into Data Science, Systems/Security classes at CS/ECE Illinois.

(3) Visual analytics "Art of HPC" on petascale network traffic exhibited at the Denver Museum of Art and Georgia World Congress Center as a part of the Supercomputing conference.

I will be a force multiplier of the business faculty, working with students and industry partners to enable innovation and technology transfers, starting with the Small Business Innovation Research (SBIR) program.

B. Teaching Expertise in Data Science and Systems Courses

I have delivered tutorials to national laboratories, served as a Guest Lecturer, and designed curricula for data-intensive courses at Illinois, in online, hybrid, and in-person formats, with students earning awards and

jobs at major tech companies (Apple, Microsoft, IBM).

(1) Large-scale, data-intensive courses include: Trustworthy and Dependable AI Systems (ECE 598), Data Science Analytics using Probabilistic Graphical Models (ECE 471), Computer Security (CS 461), Probability with Engineering Applications (ECE 313), and Computer Security with 250+ students. I contributed to those in TA, Guest Lecturer, and curriculum development roles. This background makes me well-prepared to bring real-world case studies to courses such as AI/ML for Business Analytics and Real-World Data Science for students.

(2) Proven track record of students' successes, recognized with students awarded Fiddler Innovation Fellowships. Mentored students working at senior positions at Apple, Microsoft, IBM, and national labs (Argonne, Sandia).

(3) Recognized as an Outstanding Mentor for CyberCorps Scholarship for Service (SFS) students, demonstrating a commitment to service and student career development.

As a U.S. Permanent Resident self-petitioned under EB1A (Extraordinary Ability), I can empathize with, attract, and motivate international students amid policy changes.

C. National Services and Leadership Experience

My services include serving on proposal review panels at NSF and the Department of Energy (DOE), participating in the Secure HPC working group at the National Institute of Standards and Technology, and contributing to the security posture of NSF Major Facilities, thereby exemplifying the department's leadership.

(1) National-scale leadership recognized as a TrustedCI Fellow with the NSF Cybersecurity Center of Excellence, contributing to the security posture of NSF Major Facilities through a security log analysis tutorial at Berkeley Lab, a Birds of a Feather session on Quantum-risk to Science at the National Center for Atmospheric Research.

(2) Working on policies for research security on HPC systems, in partnership with the NSF Research on Research Security Program, the NIST Secure HPC working group, and the Academic Security and Counter Exploitation (ASCE) program.

(3) Serving on panels for NSF and DOE proposals, reviewing proposals to NSF's Computer and Information Science and Engineering proposals, and the DOE's Advanced Scientific Computing Research (ASCR) program.

D. Emerging Expertise (Generative AI, Digital Twin, Supercomputing)

I maintain close connections with technical leaders (NVIDIA for GPUs), consulting (IBM Research), cybersecurity (Corelight), and clinics (Mayo and Carle). Highlights of expertise include:

(1) AI agents and LLMs: My recent work includes industry projects such as ResiliANT AIOps: Foundation-Model-Driven Resilience for Cloud Computing (IBM-Illinois Co-PI grant), which resulted in a Supercomputing publication, visual analytics showcased at the Denver Museum of Art, and an NSF award in research security.

(2) Bayesian Generative Models: Starting multiple projects on reliable and robust generative models in high-performance spaceflight computing with NASA/Jet Propulsion Laboratory.

(3) Extreme Fidelity Digital Twin: Applicable in Cardiovascular Health with Mayo Clinic and Data Center digital twin with Oak Ridge National Laboratory.

My research experience spans from fundamental computer science to applied AI/ML on supercomputer security, bridging traditional business disciplines with emerging analytics applications. I am confident I can bring both academic rigor and real-world applicability to your department's research and teaching missions.

Sincerely

/signed/

Phuong Cao

Cybersecurity Research Specialist and Research Scientist
National Center for Supercomputing Applications
1205 W. Clark St., Urbana, IL, 61801

TrustedCI Fellow
National Science Foundation
Cybersecurity Center of Excellence

References