

Dear Search Committee,

My work on *reliable and secure supercomputing* will amplify your department's efforts in AI, HPC, and Quantum Computing. My track records include multiple NSF/industry awards totaling over **\$1.8M**, resulting in interdisciplinary publications in Supercomputing, USENIX Security/NSDI, and IEEE Quantum Computing and Engineering. Successful integration of my research into your department will yield:

i) ***Advanced Curricula on Resilient and Secure AI Supercomputing***, supporting open-science research & establishing a student pipeline into critical roles at DOE, industry, and research computing institutions,

ii) ***Funding and Extreme-Scale Compute Capacity*** to accelerate interdisciplinary research in frontier areas, e.g., exascale supercomputing, HPC-Quantum Computing integration, and resilient/secure AI, and

iii) ***National Influence in Cyberinfrastructure and Research Security***, through partnership with Leadership-Class Computing Facilities, NSF Cybersecurity Center of Excellence, and industry partners.

My unique background, which combines national-scale cyberinfrastructure security research (NCSA), Internet-scale measurement experience (Akamai and Microsoft Research), and established relationships with DOE labs in exascale computing (Table 1), will realize the proposed integration.

<i>Highlight</i>	<i>Achievements</i>
Funding	Totaling more than \$1.8M in four NSF awards (FMiTF, CC*, CICI, RoRS) and IBM Research contract.
Publications	10+ peer-reviewed conference publications in Supercomputing (SC), USENIX Security/NSDI, IEEE Quantum Computing and Engineering (QCE), Dependable Systems and Networks (DSN).
Awards	<i>Best Paper Award</i> at DSN, <i>Art of HPC</i> and <i>Doctoral Showcase</i> at Supercomputing, Hackathon prize at Box.com (1 st), Salesforce \$1 Million Hackathon (10 th), <i>Trusted CI Fellow</i> with NSF.
Student's Successes	Mentored CyberCorps Scholarship for Service students (recognized as an <i>outstanding mentor</i> for a Fiddler Innovation awardee) leading to jobs in Sandia, Argonne, FAANG, etc.
Teaching	Graduate-level <i>Dependable AI Systems</i> , Undergraduate <i>Statistics</i> , <i>Computer and Network Security</i> , <i>Data Science using Probabilistic Graph Models</i> and <i>AI 101</i> for freshman (in development with NAIRR).
Software & Data Impact	Curated longitudinal performance data on petascale supercomputers (Blue Waters, DeltaAI) and mid-scale testbed (FABRIC) for open-science research, leading to preemption of ransomware attacks and recovery from system-wide outages in the NAIRR cyberinfrastructure.
Services	Proposal Review Panels (NSF, DOE); Program Committee (ACM Supercomputing, IEEE QCE); Special Issues Journal/Conf. Reviewer and Editor (IEEE TIFS, TDSC, BigData, SIGCOMM, etc.).
Authorized Work	U.S. Permanent Resident via EB1 (Extraordinary Ability) – Vietnamese national.

Table 1: Summary of Capabilities

A. Research Excellence at the Intersection of AI, Supercomputing/HPC, and Quantum Computing

I have secured over \$1.8 million in grants from the federal government and industry. As PI and Co-PI, I have published over 10 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 of granted awards on advanced cyberinfrastructure security with operational experiences of Generative AI agents, demonstrated through four 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) Bringing *art* to science through "Art of HPC" visual analytics 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. Addressing Gaps in CV

Due to a series of events, I took a full-time position at NCSA to support my family during medical emergencies. By closely collaborating with the nation's primary scientific supercomputing hub's security operators, this position enables me to apply real-world data to my PhD dissertation and has led to numerous NSF awards, as well as DOE partnerships.

D. 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.

E. Emerging Expertise (Generative AI, Digital Twin, Quantum Computing)

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 probability/statistics 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

Phuong Cao

Cybersecurity Research Specialist and Research Scientist
National Center for Supercomputing Applications
1205 W. Clark St., Urbana, IL, 61801
<https://go.illinois.edu/pcao3/>

TrustedCI Fellow
National Science Foundation
Cybersecurity Center of Excellence

<https://secpriv.lbl.gov/project/nsf-trustedci/>

References

