Institution

: **Parent Section** : **Institution**

1. Institution Name

University of Memphis

2. President of Institution

> If this information is not correct, please contact organization s CAE Tool User Access Manager to update.
>
> David Rudd
> president@memphis.edu
> 901.678.2234

> President information is not set up. If this information is not correct, please contact organization s CAE Tool User Access Manager to update.

3. Is your institution designated a minority serving institution (MSI)? If Yes Please choose from categories below:

☐ HBCU (Historically Black Colleges and Universities)

☐ PBI (Predominantly Black Institutions)

☐ HSI (Hispanic-Serving Institutions)

☐ TCU (Tribal Colleges or Universities)

☐ NASNTI (Native American Serving Non-Tribal Institutions)

☐ ANNHI (Alaskan Native or Native Hawaiian Serving Institution

☐ AANAPISI (Asian American and Native American Pacific Islander Serving Institutions)

Institution Administration

: **Parent Section** : **Institution Administration**

Annual Report Submitter Title   **Annual Report Submitter First Name**

Prof.   Dipankar

Annual Report Submitter Last Name

Dasgupta

Annual Report Submitter Phone

901-678-4271

Annual Report Submitter Email

ddasgupt@memphis.edu

CAE POC

> If this information is not correct, please contact organization s CAE Tool User Access Manager to update.
>
> Professor. Prof. Dipankar Dasgupta
> dasgupta@memphis.edu
> 9016784147

CAE Alternate POC

> Alternate POC information do not exist, please contact organization s CAE Tool User Access Manager to update.

Research Expertise

: **Parent Section** : **Research Expertise**

Using the Core Area List drop-down, identify your institution s current areas of expertise. List in descending order of expertise (No more than 10).
Area of Expertise - 1

" Cryptography ▼

Area of Expertise - 2

" Identification and Auther ▼

Area of Expertise - 3

" Authorization and Acces ▼

Area of Expertise - 4

" Wireless, link, and signa ▼

Area of Expertise - 5

" Software ▼

Area of Expertise - 6

" OS/DBMS/Network mec ▼

Area of Expertise - 8

" Forensics ▼

Area of Expertise - 9

" Cloud, Grid, distributed (▼

Area of Expertise - 10

Select Option ▼

Other

1. Intelligent tutoring systems; 2. Human-computer interaction; 3. Bio-inspired computing; 4. Cybersecurity; 5. Trustworthy AI; 6. Computer science education; 7. software engineering; 8. Biomolecular and distributed computing; 9. Data science; 10. Natural language processing; 11. Machine Learning; 12. Mobile sensor big data; 13. Behavioral privacy; 14. Socio-technical systems; 15. Computer networks; 16. Network security; 17. Multimedia communication; 18. Distributed systems; 19. Artificial intelligence/intelligent systems; 20. Internet architecture; 21. Wireless sensor networks; 22. Cyber physical systems; 23. Mobile computing; 24. Data security; 25. Blockchain; 26. Adversarial machine learning; 27. Applied cryptography

Research Funding

: **Parent Section** : **Research Funding**

Research Funding

Identify any significant funding for cyber research relevant to the current core areas/sub area of expertise (see core area list): Principles; Security Mechanisms/Functionality; Architectures; Assurance; Operations; Analysis; Non-Technical IA Issues; or Other non-identified areas.

There are four research funded projects that fit the criteria: (1) NCAE-Research on Cyber Resilient 5G-Enabled Electric Vehicle Charging Infrastructure (H98230-22-1-0326); (2) Context-Aware Authorization Framework for Smart Critical Infrastructure NCAE-C in Cybersecurity Education Research (23-5078), (3) Developing Application-specific Shared-trust Framework for Accessing Sensitive Information (H98230-21-1-0327); (4) DHS/FEMA CTG: Zero-Trust Identity & Access Management (2022-4)

NCAE-Research on Cyber Resilient 5G-Enabled Electric Vehicle Charging Infrastructure ⌃

Grant Name *

NCAE-Research on Cyber Resilient 5G-Enabled Electric Vehicle Charging Infrastructure

Grant Number

H98230-22-1-0326

Grant Period of Performance

9.16.2022 - 9.15.2024

Grant Funding Amount

$498K

Grant Description

The project s overall goal is to explore related technologies to develop a secure and trustworthy
approach for 5G-enabled electric vehicle charging station (EVCS) and its charging system. This project will significantly impact industry, academia, and society at large. In military bases, the proposed 5G-based EVCS can play a significant role in charging vehicles securely and successfully. The PIs will also engage in outreach and educational activities designed to expose diverse populations, including women, minorities and undergraduate students, to 5G-enabled EVCS and cybersecurity

Remove

Context-Aware Authorization Framework for Smart Critical Infrastructure NCAE-C in

Cybersecurity Education Research

Grant Name *

Context-Aware Authorization Framework for Smart Critical Infrastructure NCAE-C in Cybersec

Grant Number

23-5078

Grant Period of Performance

10.1.2022 - 9.30.2024

Grant Funding Amount

$140K

Grant Description

The University of South Carolina (lead institute), the University of Memphis, and The Citadel propose a joint research project to develop a secure authorization framework for critical infrastructure components. International conflicts make the United States of America a prime target for state sponsored cyber-attacks. As cybersecurity threats

Remove

Zero-Trust Identity & Access Management

Grant Name *

Zero-Trust Identity & Access Management

Grant Number

2022-4

Grant Period of Performance

9.1.2022 - 8.31.2025

Grant Funding Amount

$450K

Grant Description

The goal of this project is to increase the understanding of Zero Trust methodology, principles and implementation and also to prepare organizations to face existing threats and adapt to new threats in the future. CfIA will develop a new 5-hour web-based course titled, Zero Trust: Identity & Access Management, to serve approximately 400 individuals and help state, local, tribal and territorial governments and private industry administrative and IT personnel implement organizational policies, procedures

Remove

Developing Application-specific Shared-trust Framework for Accessing Sensitive Information

Grant Name *

Developing Application-specific Shared-trust Framework for Accessing Sensitive Information

Grant Number

H98230-21-1-0327

Grant Period of Performance

8.1.2021 - 7.31.2023

Grant Funding Amount

$251K

Grant Description

Center for Information Assurance director Professor Dipankar Dasgupta received a $251K grant from the National Centers of Academic Excellence in Cybersecurity for Developing application-specific shared-trust framework for accessing sensitive information.

Remove

Multidisciplinary Cybersecurity Program for Critical Infrastructure Protection ^

Grant Name *

Multidisciplinary Cybersecurity Program for Critical Infrastructure Protection

Grant Number

H98230-21-1-0319

Grant Period of Performance

8.20.2021 - 12.31.2023

Grant Funding Amount

$2M

Grant Description

The overall project goal is to design and develop a multi-disciplinary critical infrastructure cybersecurity program addressing the technical needs of public utility operations and emergency decision-makers. A successful outcome of this project will create a strong southeast regional coalition, leveraging the NCAE s expertise in cybersecurity to assist NCAE-C students (the future workforce), state and local government and critical infrastructure industry partners in contending with evolving threats. CfIA Co-Directors Dr. Dipankar Dasgupta (Computer Sc) and Dr. James

Remove

Cybersecurity Impact Analysis for End Users Security and Privacy ^

Grant Name *

Cybersecurity Impact Analysis for End Users Security and Privacy

Grant Number

2021-3

Grant Period of Performance

9.1.2021 - 8.31.2024

Grant Funding Amount

$600K

Grant Description

The Center for Information Assurance received a $600K grant from DHS/FEMA to develop cybersecurity training courses on Remote Home Office (RHO) security and End Users Security and Privacy (ESP). The UofM portion of the DHS/FEMA grant is led by Professor James McGinnis (Engineering Technology), and the grant is part of a multi-

Remove

Scholarship for Services (SFS) ⌃

Grant Name *

Scholarship for Services (SFS)

Grant Number

2146427

Grant Period of Performance

2.1.2022 - 1.31.2027

Grant Funding Amount

$3.8M

Grant Description

A $3.8 million Cybersecurity Education Grant from National Science Foundation (NSF). The five-year project, titled CyberCorps Scholarship for Service: Developing the Cybersecurity Workforce in West Tennessee, Mississippi, and Arkansas will recruit four cohorts of scholars from the Department of Computer Science, Department of Business Information Technology, College of Engineering, Department of Criminal Justice and other UofM units. Priority will be given to underrepresented students such as women,

Remove

GenCyber Summer Boot Camp for High School Students

Grant Name *

GenCyber Summer Boot Camp for High School Students

Grant Number

H98230-22-I-0109

Grant Period of Performance

3.01.2022 - 2.28.2023

Grant Funding Amount

$100K

Grant Description

The Department has received a new one-year, $100K cybersecurity education grant from the National Security Agency. Part of the NSA s GenCyber program, the project will create an integrated curriculum, in consultation with a K 12 pedagogical expert, focused on incorporating fundamental cybersecurity concepts with their applications to

Remove

Designing Machine Learning-based Solutions for APT

Grant Name *

Designing Machine Learning-based Solutions for APT

Grant Number

MSA 12-1048-013

Grant Period of Performance

8.1.2022 - 7.31.2025

Grant Funding Amount

$397K

Grant Description

UofM s Dr. Kan Yang (PI) and Dr. Xiaofei Zhang (Co-PI), two assistant professors in the Department of Computer Sciences, have been awarded funding from FedEx Service Inc. to develop advanced machine learning-based solutions to enhance the enterprise cyber analytic defense ecosystem. The project, entitled Designing Machine Learning-based Solutions for APT Detection, will explore the recent advancement of machine

Remove

Add New Grant

Grants

Identify any significant grants for cyber

New Grant

Grant Name

Grant Number

Grant Period of Performance

Grant Funding Amount

Grant Description

Add New Grant

Add New Grant

Outreach / Professional Development

: Parent Section : Outreach / Professional Development

1. Professional Development

Provide separate examples of professional development opportunities provided to faculty and students since your last annual report / application.

Evidence files can be fliers, posters, letters, attendance records, or other evidence of professional development for faculty and students (in PDF).

PDF

Choose Files   No Files Selected

Name	Size	Action
agenda_workshop_smartgrid.pdf	**111020**	Delete

2. Outreach Activities

2a. Provide evidence of how the institution has shared cyber related curriculum and/or faculty with other schools, to include K-12 schools, community colleges, technical schools, minority colleges/universities to advance cyber defense knowledge since your last annual report / application. Identify specific materials provided, to whom the material was provided, when and for what purpose. Any additional supporting documentation of this exchange, such as emails, formal meeting notes, links to material on accepting parties website, etc. is encouraged (in PDF).
Provide evidence of how the institution has shared cyber related curriculum and/or faculty with other schools, to include K-12 schools, community colleges, technical schools, minority colleges/universities to advance cyber defense knowledge since your last annual report / application. Identify specific materials provided, to whom the material was provided, when and for what purpose. Any additional supporting documentation of this exchange, such as emails, formal meeting notes, links to material on accepting parties website, etc. is encouraged (in PDF).

Choose Files   No Files Selected

Name	Size	Action
cybersecuritysummit2022-report.pdf	12371430	Delete

2b. Provide evidence since your last annual report / application that the institution has participated in CAE events such as: CAE Community Symposium, CRRC workshops for applying institutions, CAE Tec Talk/Forum used in classroom, collaboration on grants with CAE institutions (in PDFs).

PDF1

Choose Files   No Files Selected

Name	Size	Action
iot_security_workshop_agenda.pdf	1505043	Delete

PDF2

Choose Files   No Files Selected

Name	Size	Action
UofSC-UofM-Citadel-Executive-Summary_Final.pdf	70630	Delete

PDF3

Choose Files   No Files Selected

Name	Size	Action
San Antonio CAE-CD Peer Review.pdf	156328	Delete

2c. Provide evidences since your last annual report / application that faculty members from the institution has contributed to the CAE community such as: served as PoS Validation and/or CAE-C Designation mentors, reviewers, members of the CAE Working Groups, presented in CAE Community Symposiums, CRRC workshops, CAE Tech Talk/Forum (in PDFs).

PDF1

Choose Files   No Files Selected

Name	Size	Action

Name	Size	Action
Speaker and Panelist Biographies - Cyber Resiliency for Critical Infrastructure (1).pdf	**10974585**	Delete

PDF2

Choose Files   No Files Selected

Name	Size	Action
CERIAS _ Adaptive Multi-Factor Authentication & Cyber Identity - Purdue University.pdf	**227999**	Delete

PDF3

Choose Files   No Files Selected

Name	Size	Action
UofSC-UofM-Citadel-Executive-Summary_Final.pdf	**70630**	Delete

2d. Provide evidence since your last annual report / application of faculty members collaborating with current CAE-C institutions on research, grants, course development, etc. (in PDF).

Choose Files   No Files Selected

Name	Size	Action
DoD University Consortium for Cybersecurity - Division of Research and Innovation - The University of Memphis.pdf	**297908**	Delete

2e. Provide evidence since your last annual report / application of faculty members/employee sponsorship or oversight of students for Cyber events for the community at large. Events could include Cyber awareness and education for local schools, adult education centers, senior centers, camps, first responder training and the surrounding community (in PDF).

Choose Files   No Files Selected

Name	Size	Action
2022_cyber_ambassador_techcamp_summary.pdf	**538819**	Delete

2f. Provide evidence since your last annual report / application on how the institution works with employers and students to support placement for cyber related internships and jobs, such as via institutional Career Development Services (i.e. HandShake) and industry events on-campus (in PDF).

Choose Files   No Files Selected

Name	Size	Action
Raymond James Capture the Flag_Agenda for Faculty Advisors_10-2022.pdf	**161396**	Delete

2g. Provide evidence since your last annual report / application of obtaining input on curriculum to meet industry needs (in PDF).

Choose Files   No Files Selected

Name	Size	Action
ABMeeting221118.pdf	**152128**	Delete

Institution Reflective of the CAE Designation

: Parent Section : Institution Reflective of the CAE Designation

Institution Successes & Achievements

Since the institution s last designation application - Describe activities that represent successes and achievements of the program(s) reflective of the CAE designation / POS Validation such as scholarships, outreach, partnerships, awards, conference participation, etc.

> Dr. Kan Yang, University of Memphis CfIA Associate Director, received NSF's CyberCorps Scholarship for Service grant. During the Fall 2022 semester, three students entered the program: 1 undergraduate, 1 accelerated bachelors & masters, 1 doctor of philosophy. During the Spring 2023 semester, four additional undergraduate students entered the program.

Designation Return on Investment

Identify any opportunities, successes and/or achievements, grants specifically resulting from the institution s designation as a CAE.

> Dr. Hasan Ali and Dr. Dipankar Dasgupta received NSA grant on "NCAE-Research on Cyber Resilient 5G-Enabled Electric Vehicle Charging Infrastructure." Additionally, Dr. Dipankar Dasgupta was an University of South Carolina subaward recipient for the "Context-Aware Authorization Framework for Smart Critical Infrastructure NCAE-C Cybersecurity Education Research."

CAE Community Contributions

Check all that apply to the institution s specific contributions to the CAE Community:

- ☑ Attendance at CAE Community Meetings
- ☑ CAE Mentor / Reviewer
- ☐ Participation in CAE Working Groups (name working group)
- ☑ CAE Research Collaborations (state collaboration information)
- ☑ CAE Forum / Tech Talk contributor (date presented / topic)
- ☐ CAE Regional Hub (CRH) or CAE National Resource Center (CNRC)
- ☐ Participation in KU development and refinement
- ☑ Other (provide contribution information)

Cybersecurity Impact Analysis

Additional Information

Institution may use this section to provide any additional information not previously mentioned in this report pertinent to the CAE program.

It should be noted that the "Organization Details - President of Institution" was updated, but has of yet to be migrated to the "I. Institution: 2. President of Institution" tabs of the Annual Reports. The issue has been brought to the attention of the CAE Application Portal developers. Additionally, please note the following: (1) The UofM's cybersecurity club is called the Cyber Tigers. It's president's name is Spencer Tartera. (2) Tony Pinson, UofM CfIA Project Coordinator, attended CAE Program Development Advisor Workshop on January 27, 2023. (3) Tony Pinson, UofM CfIA Project Coordinator, is serving as a CAE Mentor for Temple University's Cyber Program. (4) Tony Pinson, UofM CfIA Project Coordinator, attended the FDA: Automobile Security - Car Penetration Testing/Mall of America event on August 10, 2022.