CYBERSECURITY RESEARCH AWARD

DARKMATTER

Frequently Asked Questions

1. **What is the Cybersecurity Research Award, and how did it originate?**

- DarkMatter's key strategic pillars include cybersecurity research and knowledge transformation. The cybersecurity research award will bring together an international and local community of experts, with new ideas for cybersecurity, while also promoting advancement of knowledge and product innovation. This year's theme for the research award focuses on **Cybersecurity Threats to Smart** Cities aiming for increasing the reliability and, therefore, the adoption of Smart Cities solutions.
- The Cybersecurity Research Award will bring together university students and principal investigators to present their original research ideas during the **HITB$^+$ Cyber Week UAE 2019 event,** which combines over 20 activities and programs simultaneously across a six-day period from October 12th – 17th 2019. One of the main programs delivered during HITB$^+$ Cyber Week is the **University Pavilion,** which showcases cutting edge research award and career fairs related to cyber security.
- The Cybersecurity Research Award is a pilot program where one team will be selected and awarded a total grant of **USD 1.5M over a 3-year period.** The winning team will be announced in May 2020. Post its completion, learnings from the program will be taken to incorporate them for an Annual UAE Cybersecurity Research Award.

2. **Who is leading the grant? Who are the partners?**

- The grant is led by DarkMatter with Khalifa University (KU) as their strategic partner and Dubai Electronic Security Center (DESC) as their advisory partner. Additionally, Mohammed Bin Rashid Al Maktoum Knowledge Foundation (MBRF), University of Sharjah, Abu Dhabi Polytechnic, and NYU Abu Dhabi are knowledge partners for this initiative.

3. **Why is the Cybersecurity Research Award so important?**

- The main objectives of the Cybersecurity Research Award are to advance techniques, technology and implementation of cybersecurity practice, increase the reliability, and therefore, the adoption of Smart Cities solutions globally. This research award is a global opportunity to advance Smart Cities and cybersecurity technologies.

- Smart Cities Security Perspective: To ensure secure and resilient smart cities, it is fundamental that we are able to avoid and respond to threats, and it is important for Smart Cities to understand and identify vulnerabilities and to have reliable solutions.

- Academic Research Perspective: This initiative will help advance knowledge, the sharing of innovative research, and to bring international recognition to the potential of research in cybersecurity for Smart Cities to improve citizens' security around the world. This will also improve collaboration between local and international institutions resulting in improving local expertise and talent development.

- United Arab Emirates Perspective: A national mandate for the UAE is to promote and progress the implementation of its safe and smart cities strategy. The research award will help in establishing Dubai and Abu Dhabi as models for safe and functional Smart Cities. Dubai and Abu Dhabi are already the highest ranked cities in the Middle East and Africa for deployment of the Smart City applications and there is a significant opportunity to improve (according to the McKinsey Global Institute, June 2018; McKinsey Global Institute CityScope database).

4. How much funding is available?

- One team will win the total grant funds of USD 1.5M that will be dispersed across a period of 3 years (not exceeding USD $500,000 per year).
- Continued support will be contingent upon a satisfactory outcome of progress reports every 6 months. DarkMatter will cover the travel and lodging costs of this formal visit twice a year.

5. How many grants are being awarded?

- This is a pilot program, one team will be selected and awarded a total grant of USD 1.5M over a 3-year period.

6. Once selected to present at the poster talk, who pays for the travel/lodging expenses to the UAE for the presentation?

- DarkMatter will cover the travel and lodging expenses for all teams chosen to participate in the poster talk in October 2019 during the **HITB$^+$ CyberWeek event.**

7. What is the theme for the Cybersecurity Research Award?

- Theme: Cybersecurity Threats to Smart Cities
- Proposed research topics can tackle any of the following Initiative by examining eight **applications** of Smart Cities:

i. Security
ii. Energy
iii. Healthcare
iv. Water
v. Economic development and housing
vi. Engagement and community
vii. Mobility
viii. Waste

- The **technology focus** of the proposed research may include one or more of the following:
  i. Artificial Intelligence (Machine Learning)
  ii. Blockchain/Cryptography (e.g. side channel analysis techniques and post quantum crypto)
  iii. Big Data
  iv. IoT
  v. Edge Computing
  vi. Mobile and the cloud

8. How do I apply for the program?

- All required documentation should be sent through email at csra@darkmatter.ae.
- The award will be selected by a rigorous, three-stage merit review process, and announced in May 2020:
  - Pre-Proposal is REQUIRED – Submission deadline for pre-proposals is August 30, 2019
  - Poster Talk is INVITATION ONLY – Deadline for accepting poster talk invitations is September 26, 2019
    i. Selected teams from pre-proposals stage will be flown to Abu Dhabi, UAE to present their poster talks during HITB^{+} CyberWeek 12-17 October 2019 at the illustrious Emirates Palace.
    ii. Travel and lodging costs will be covered by DarkMatter.
  - Full Proposal is INVITATION ONLY – Submission deadline for full proposals is February 18, 2020

9. What is the deadline for proposals?

- Pre-Proposal is REQUIRED – Submission deadline for pre-proposals is August 30, 2019
- Poster Talks is INVITATION ONLY – Deadline for accepting poster talk invitations is September 26, 2019
- Full Proposal is INVITATION ONLY – Submission deadline for full proposals is February 18, 2020

10. Does the Cybersecurity Research Award grant deadline extensions?

- No, all submission deadlines are final, and no extensions will be granted.

11. What is the role of the Cybersecurity Research Award (CRA) committee?

- The CRA committee will be responsible for overseeing the proposal submission process, review of conflicts of interests (COIs), panel selection and assignments, and overseeing the review and award processes.
- The CRA committee will rely on a merit review process that incorporates consideration of both the technical aspects of a proposed project and its potential to contribute more broadly to the security of Smart Cities.
- The CRA committee will make every effort to conduct a fair, competitive, transparent merit review process for the selection of projects. In all cases, the decision of the CRA committee is final.

12. Can the Cybersecurity Research Award committee provide individual support to applicants?

- While the CRA committee is happy to answer any questions about the submission procedure, the Program Policy does not allow the committee to provide individual support regarding the project ideas, pre-proposals, poster talks, or full proposals. In particular, the committee is not allowed to give opinions on the projects or recommendations for collaborations with local institutions.

13. Who may submit proposals?

- Domestic (UAE) or foreign academic universities, research institutions, and think tanks (not for profit organizations that focus on research) are eligible to receive this cooperative agreement award.
- Research entities and labs that are associated with companies are not eligible to participate for this award.
- All eligible entities must clearly demonstrate that they have access to facilities and infrastructure necessary to carry out the proposed project and agree to the fiscal arrangements that the Cybersecurity Research Award (CRA) committee requires to clearly prove the ability to responsibly manage the funds.

14. Who may serve as Principal Investigator and Co-Principal Investigator?

- The Principal Investigator (PI) must have substantial research and management experience in a field of science and/or engineering to lead the project.

- Co-Principal Investigators (Co-PIs) may share in the responsibility of the scientific or technical direction of the project. The first name listed on the application will serve as the primary liaison to Notification by the Cybersecurity Research Award (CRA) committee and have responsibility for the project management and the submission of reports.

15. Is there a limit on number of pre-proposals per organization?

- There is NO LIMIT on the number of pre-proposals that can be submitted to this competition. However, it should be noted that any one organization may only receive one award per competition cycle.

16. Is it possible to submit a joint proposal with DarkMatter?

- Employees of DarkMatter are not eligible to apply for this program or to serve as a project Principal Investigator or Co-Principal Investigator individually or jointly.

17. Do you encourage cooperative projects between different universities?

- Yes, active cooperation with and among universities and research institutions for the benefit of the project is encouraged. Engagement with UAE institutions is particularly encouraged.

18. Where do I submit my pre-proposal cover page and pre-proposal?

- Please send in your pre-proposals and cover page through email at csra@darkmatter.ae.

19. Why did I not receive a confirmation after submitting my pre-proposal cover page and pre-proposal?

- If you have not received a confirmation email after submitting the pre-proposal, please contact us at csra@darkmatter.ae.

20. Can I also submit my proposal by mail or fax?

- Only submissions sent through email at csra@darkmatter.ae are eligible.

21. What is the process after I submit a pre-proposal?

- All awards will be selected by a rigorous, three-stage merit review process, and teams will be notified of their advancement in a timely manner on the following dates:

i. Notification of invitation for Poster Talk presentations: September 19, 2019
ii. Deadline for acceptance of invitation for Poster Talk presentations: September 26,2019
iii. Poster Talk presentations: October 2019
iv. Notification of invitation to submit Full proposal: October 31, 2019
v. Deadline for submission of Full proposal: February 18, 2020
vi. Notification of FINAL awardee: May 2020

22. How will I be notified of a decision?

- Teams/projects advancing to the next stage will receive an email indicating the invitation.

23. Who will evaluate the pre-proposals, poster talks, and full proposals?

- The Cybersecurity Research Award (CRA) committee will work with independent reviewers and willy rely on a merit review process that incorporates the consideration of both technical aspects of a proposed project and its potential to contribute more broadly to the security of Smart Cities. **At least two independent reviewers** will review each pre-proposal.

  The reviewers will be instructed to base their critique and scores solely on the written materials provided in the application. Therefore, links to URLs or other supplementary information not otherwise specifically allowed for this competition shall not be used as part of the evaluation process.

  The independent reviewers will be selected based on the following criteria:

  i. Scientific and engineering expertise pertinent to the submitted proposals to ensure ability to evaluate competence, significance and impact of the proposed activity;
  ii. Generalized knowledge of cybersecurity and Smart Cities;
  iii. Extensive knowledge of the scientific and engineering enterprise, including managing and evaluation of large research projects. All reviewers will be instructed in the program's confidentiality, conflict of interest, and ethics guidelines and required to sign confidentially and conflicts of interest forms to indicate their assent to abide by these policies.

  The Cybersecurity Research Award (CRA) committee will be responsible for overseeing the proposal submission process, the review of cases with potential conflicts of interests, the panel selection and assignments, and the award processes. The CRA committee makes every effort to conduct a fair, competitive, transparent merit review process for the selection of projects. In all cases, the decision of the CRA committee is final.

24. Will feedback be provided in case of rejection of pre-proposals?

- Feedback will be provided by each reviewer at every stage of the Research Award
  - i. Pre-proposals (based on documents submitted before August 30, 2019)
  - ii. Poster Talks (based on the presentations done during HITB+ CyberWeek in October 2019)
  - iii. Full Proposals (based on the documents submitted before February 18, 2020)

25. How will the pre-proposals be evaluated?

- The evaluation of the pre-proposals will be based on limited written materials.
- Pre-proposal evaluations will be based on the following criteria:
  - i. Research excellence, impact and quality;
  - ii. Experience and/or expertise of the proposers, and potential for success;
  - iii. Potential to enhance or transform the cybersecurity research community and industry, specifically in the context of security for Smart Cities.

26. How will the poster talks be evaluated?

- The poster talks will be evaluated by the following criteria:
  - i. Does the research have Intellectual Merit (the potential to advance knowledge) as well as Broader Merit (the potential to benefit society and to contribute to the achievement of specific, desired societal outcomes)?
  - ii. Does the poster/presenter clearly identify what will change/improve as a result of the research activities?
  - iii. Is the proposed strategy appropriate for addressing a cybersecurity threat to the identified specific smart city application and technologies?
  - iv. Is the proposed timeline and budget/resources appropriate?
  - v. Are the graphics or visual representations of the data compelling and easy to interpret? Is the overall poster aesthetically pleasing?
  - vi. Does the presenter demonstrate full knowledge of the material? Is the presenter able to explain and elaborate on expected questions?

27. How will the full proposals be evaluated?

- The full proposals will be evaluated based on the following components:
  - i. Overall Scientific & Technical Merit, Significance, and Innovation – 30%

- How does the proposed activity address important challenge(s), gaps in knowledge and/or critical barriers to the progress of the field?
- If the aims of the proposal are achieved, how will scientific knowledge, techniques and technologies be advanced?
- Is the research based on sound and testable physical hypotheses - and if so, how?
- Does the application clearly challenge or seek to validate current research or technology paradigms - and if so, how?
- How are the concepts, approaches and technologies proposed novel either to the field or in a broad sense?
- How significant are the potential contributions with regard to impact on the stated program goals?
- What are the broader impacts/benefits for the field of cybersecurity?

ii. Approach – 20%
- How well conceived and organized is the proposed activity?
- Does the plan incorporate a mechanism to assess success?
- How well does that plan show alignment with local universities?
- If experimental, will the design adequately test, and the evaluation plan adequately validate, the hypotheses?
- Are the computational models, laboratory equipment, or field experimental equipment and infrastructure supported with appropriate and well-planned commitments?
- Is there a correct use of statistics as a supporting tool?
- Is the data plan consistent with the research proposed and with the solicitation's fundamental data principles?
- Does the application identify major risks and, if so, are plans in place to minimize and/or mitigate?
- Does the approach identify and account for any potential environmental and social consequences?

iii. Investigator/Team – 20%
- How well qualified is the proposer (individual or team) to conduct the project?
- If early stage researchers are involved, how adequate is their training and experience?
- For established researchers, have they demonstrated an ongoing record of accomplishments that have advanced the field?
- If the project is collaborative or has co-PIs, do the researchers have complementary and integrated expertise and to what extent does the collaboration provide added benefit?
- Is the leadership approach, governance, and management structure appropriate for success of the project?

- What are the features of the management plan that will ensure success?

iv. Resources and Budget – 20%

- Have additional sponsors or means of support been identified to complement the proposed project budget?
- Does the research team have access to adequate facilities and infrastructure to conduct the proposed research, and has the team demonstrated the necessary institutional commitment(s) to be successful?
- Are the project costs complete and fully documented?
- Is the budget fully justified and reasonable in relation to the proposed research?
- Are additional resources and in-kind contributions stated in the proposal logical, justified, and provide clear additions to the project impact? (e.g., does the award leverage other research activities or funding to increase its impact?)

v. Capacity Building – 10%

- What is the potential to increase the visibility and reputation of the field, or to grow the field regionally and/or globally?
- Are there educational and experiential opportunities for graduate students, new researchers, and/or technical workforce?
- How is capacity building integrated within the research plan and what is the plan for knowledge transfer within the DarkMatter team?
- Partnership with local universities is encouraged

28. Are all submissions treated equally regardless of their origin?

- Yes, the Cybersecurity Research Award program actively seeks the participation of research and scientific institutions worldwide. The independent reviewers will evaluate all proposals strictly on merit and according to their scientific potential.

29. Do you prefer one technology or methodology to others?

- We are open to any innovative research ideas related to cybersecurity. Please refer to the “Terms and Conditions” document mentioned in the RFP for more details.

30. Who will have ownership of the IP?

- The institution/s working on the product/idea will own the IP. However, DarkMatter will have first right to license the product/idea.

31. What constitutes a conflict of interest?

- As the Principal Investigator (PI), all conflicts of interest must be mentioned in the pre-proposal. Possible conflicts of interest are defined as follows:

  i. Individual conflicts of interest include, but are not limited to:
     - Ph.D. dissertation or thesis advisors or advisees
     - Collaborators or co-authors, including postdoctoral researchers, for past 48 months
     - Co-editors within the past 24 months
     - A spouse or close relative
     - Any other individuals with whom you believe may present a circumstance where your impartiality may be questioned.

  ii. Institutional conflicts of interest include, but are not limited to:
     - Advisory committees
     - Boards
     - Current or prospective partner or employer
     - Stock owned
     - Received money in the past year- honoraria or travel expenses
     - Other recent or on-going financial ties

32. What happens if a conflict becomes apparent to a proposal reviewer after being assigned a proposal to review?

- It is the responsibility of the Principal Investigator (PI) to clearly explain all known conflicts of interest in the pre-proposal.
- The committee is aware of the fact that conflicts of interest might become apparent after proposal review assignments are made. If a conflict of interest becomes apparent at any time after review assignments are made, it is the obligation of the reviewer to inform the committee immediately so that the respective proposal can be reassigned.

33. Are the Principal Investigators (PIs) allowed to suggest ad-hoc reviewers for their respective pre-proposals and full proposals?

- Yes, PI’s may suggest ad-hoc reviewers, it is encouraged. However, it is at the discretion of the committee to accept these suggestions.

34. Can the proposal budget’s 20% indirect costs limit be waived or modified?

- No, waiving or modifying the 20% indirect cost rule is not possible. Further questions regarding overhead should be directed to csra@darkmatter.ae.