सत्यमेव जयते

Ministry of Electronics & Information Technology
Cyber Security R&D Division
Call for proposals under Cyber Security R&D Division
Last Date of Submission: Nov 20, 2018

Background

Innovation in cyberspace has proliferated to an extent where it is touching almost every facet of individuals, businesses and government. Government and industry are leveraging capabilities of digital technologies for delivering services, improving performance and for many other inherent benefits of cyber technologies. India, through its initiatives such as Digital India, Make in India, Start-up India - Stand-up India is also stimulating the pace of development and adoption of technologies.

Such innovations, while opening plethora of opportunities on one hand, also open the avenues for illegitimate elements in the ecosystem to exploit them for malicious purposes, on the other

Considering the criticality of services being delivered & the sensitivity of the data being involved, severity & scope of the impact in case of any breach or attack in Cyberspace could be immense.

Strengthening the cybersecurity posture of the nation as a whole is certainly need of the hour. This includes building capabilities and capacities of individuals, industry and government, and MeitY is cognizant of this. Considering the importance, MeitY has already taken several initiatives to strengthen the cyber security posture of the nation and ensure protection of the sovereignty of the nation in the cyberspace and also protect the rights of the citizens

1. Vision and Goals

Cyber Security R&D is one of the major pillars identified for securing Cyber space with focus on promotion of R&D, demonstration, proof of concept and establishment of test beds for enhancing skills and capabilities in the country in this critical domain.

The Cyber Security R&D Programme is aligned with the National Telecom Policy Vision 2022 which has vision of “Ensuring Digital Sovereignty, Safety and Security of Digital Communications” and MeitY’s initiative of “Cyber Surakshit Bharat”

India needs to build a robust research base for technology and product development, testing, evaluation and certification framework and

standardization to enhance cyber security posture of the country in a well-rounded fashion

The Cyber Security Strategic Research programme should be based on the following 4 principles:

- Detect
- Deter
- Protect
- Adapt

Government is closely working with Academia and R&D labs and pursuing research and development work which is suitable to meet the security challenges faced in various cyber security domains.

2. Category of Research

The Research and Development may be categorized in 3 different time scales

(1) Near term: 1-2 years

(2) Medium Term: 2-5 years

(3) Long / Future Terms: 5-7 years

The Research and development activity should also be aligned to incubate and develop products/market solutions in collaboration with industry players, particularly MSMEs and Start-ups.

Thematic Areas

The Cyber Security Research agenda may be developed for the following domains:

1. Cryptography and cryptanalysis including the Post Quantum Cryptography and Quantum Cryptanalysis including (i) quantum key distribution (QKD) and (ii) quantum random number generators (QRNG)
2. Critical Infrastructure Security (SCADA and IIOT), including Embedded System Security
3. IoT and Connected Devices Security including 5G , Cloud , Edge and Fog Computing Security
4. BlockChain Security.
5. Network and System Security AI in Information Security including Threat Intelligence
6. Digital Forensics and Monitoring tools
7. Breach prediction, response and rapid mitigation
8. Vulnerability prioritization, Remediation & Assurance
9. Advanced Analytics for Cyber Security
10. Application Security - Correlation/ Prioritization, Contextual S/W Analysis, Rapid Mitigation
11. Security enforcement in high speed traffic

12. Malware analysis Software Testing, including Protocol testing Software Defined Network and Network Function Virtualization Security Social Media Security.
13. Fintech Security

In addition to the above, it is also necessary to develop and strengthen security testing processes by:

1) Enhancing institutional capacity to perform testing, including establishing domestic testing hubs and laboratories with state-of-the art facilities.

2) Establishing comprehensive security certification regime based on global standards

3) Formulating a policy on encryption and data retention, by harmonising the legal and regulatory regime in India pertaining to cryptography with global standards, as applicable to communication networks and services

Proposals may also include aspects regarding testing, evaluation and certification as mentioned above.

Who Can Apply

Research and Development proposals from single institution and Consortium Mode (preferred) are invited for the above mentioned areas with a special focus on technology / product development and pilot deployment with active involvement and participation from user organizations. Involvement of SMEs/Industry partner in the conceptualization phase is encouraged.

Last Date of Submission:
Last date for submission: The last date for on-line submission of the proposals is **20/11/2018** and a hard copy/physical copy (3 copies) of the proposal by post should reach to MeitY on the date of on-line closure. No proposals will be accepted after the last date. Only those proposals received both online and hard-copy within the stipulated time will only be considered.

The Project proposals may be submitted to:
Shri Arvind Kumar, Sr. Director and Group Coordinator
Cyber Security R&D Division
Ministry of Electronics & Information Technology, Government of India
Electronics Niketan
6 CGO Complex
Lodhi Road
New Delhi 110003 .e-mail: **csrd@meity.gov.in** +91-11-2436 4754