इलेक्ट्रॉनिकी एवं
सूचना प्रौद्योगिकी मंत्रालय
MINISTRY OF
ELECTRONICS AND
INFORMATION TECHNOLOGY

सत्यमेव जयते

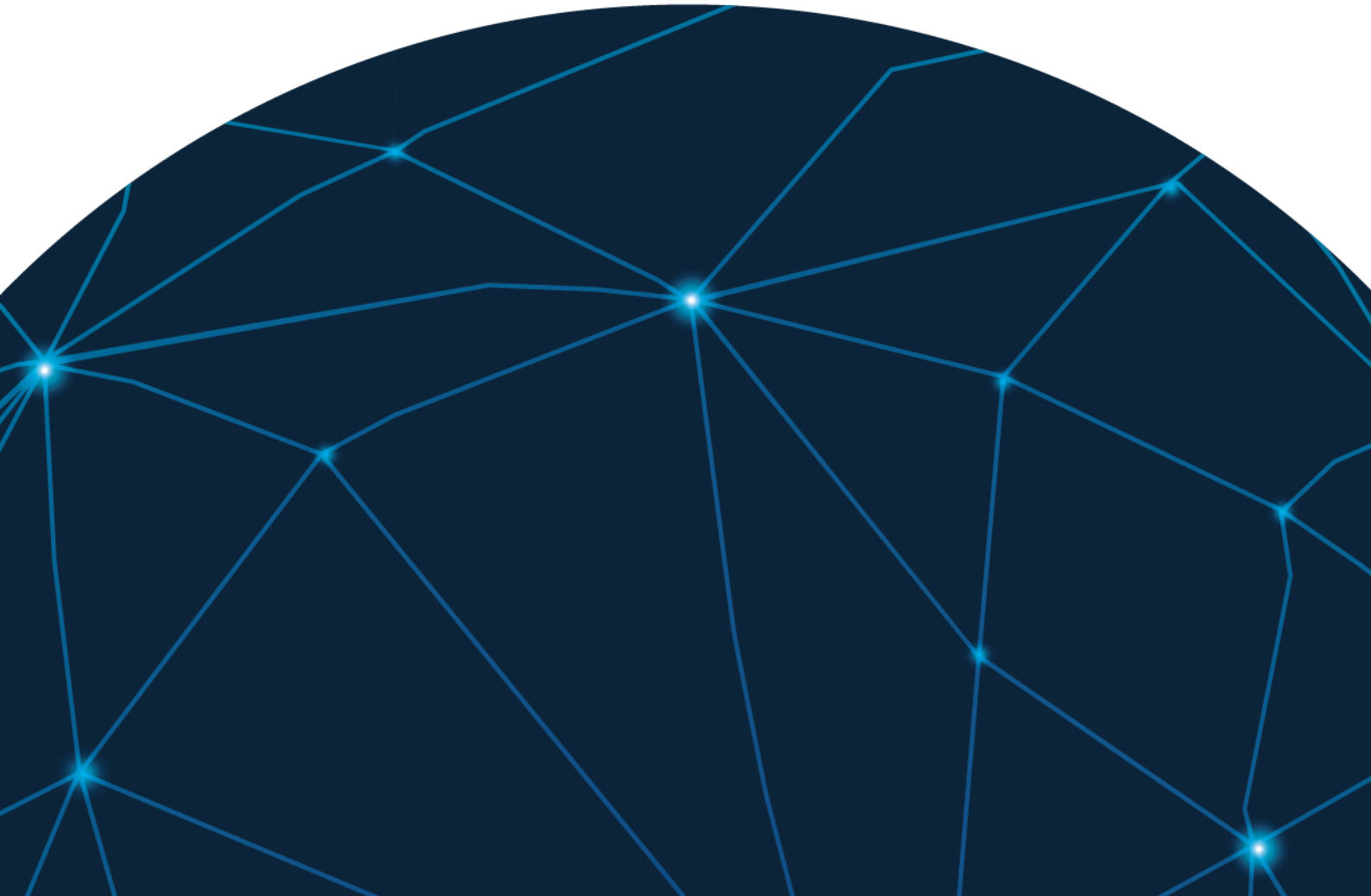
www.isea.gov.in

DSCI
PROMOTING DATA PROTECTION
A nasscom Initiative

RULEBOOK

CYBER SECURITY INNOVATION CHALLENGE 1.0

Under the Aegis of ISEA Project, MeitY



Contents

About ISEA

Information Security Education and Awareness (ISEA) is an initiative of Ministry of Electronics and Information Technology (MeitY), Government of India for generating human resources in the area of Information Security and creating general awareness on Cyber Hygiene/Cyber Security among masses. ISEA project is aimed at human resources development for safe, trusted, and secure cyber space across the nation. The project is implemented through select 50 institutions in a hub-n-spoke mode, comprising premier academic institutions (IITs, NITs, IIITs, etc.), Autonomous Organizations of MeitY (C-DAC & NIELIT) and Technical Universities. C-DAC Hyderabad is functioning as a nodal agency and PMU under the project. Data Security Council of India (DSCI) is functioning as the nodal agency for overall coordination and management of ideation & innovation activities under the project. More details of the project are available at https://isea.gov.in/

About Data Security Council of India (DSCI)

The Data Security Council of India (DSCI) is a not-for-profit, industry body on data protection in India, setup by NASSCOM, committed to making the cyberspace safe, secure and trusted by establishing best practices, standards and initiatives in cyber security and privacy. To further its objectives, DSCI engages with governments and their agencies, regulators, industry sectors, industry associations and think tanks for policy advocacy, thought leadership, capacity building and outreach activities. DSCI is acting as a nodal agency for the ideation and innovation component, leading the overall coordination and management of the Innovation Challenge under the ISEA Project. The initiative encourages collaboration between academia, industry, and government.

About Cyber Security Innovation Challenge 1.0

The Cyber Security Innovation Challenge 1.0 (CSIC 1.0), under the Information Security Education and Awareness (ISEA) Project of the Ministry of Electronics and Information Technology (MeitY), Government of India is aimed to nurture cutting-edge indigenous innovations in cyber security by students and researchers. It plays a pivotal role by fostering a product-building mindset from the ideas of early stage. Through its five-stage structure, CSIC 1.0 nurtures promising ideas from conception to Minimum Viable Product (MVP), strengthening India's cyber security innovation ecosystem.

1. Objectives of the Cyber Security Innovation Challenge 1.0

- **Building a Robust Cyber Security Innovation Ecosystem:** The challenge will lay the foundation for a sustainable ecosystem that encourages continuous innovation in cyber security. By giving targeted support to the student-led ideas and student-led startups through MVP development support and industry expertise and mentorship, this will create a security product building mindset from the early-stages.

- **Generating Sector-Relevant, Scalable Cyber Security Solutions:** The focus on domain-specific problem statements ensures the development of practical, deployable solutions, catering to a specific industry. Participants will have an opportunity to design products, tools and frameworks tailored to India's critical sectors, including BFSI, telecom, healthcare, and emerging digital infrastructure.

- **Fostering Collaboration between Industry, Academia, and Students:** The challenge creates a platform for meaningful engagement across stakeholders. Industry experts will mentor participants, academic institutions will contribute research-driven insights, and students will get to build a product/tool/framework potentially leading to a startup.

2. Problem Statements

S. No.	Area	Problem Statements
1	Computer & Network Security	Cloud Misconfiguration (Security Scanner)
2	Mobile Device Security	Ransomware Early Warning System for Android Devices
3	Systems & Software Security	DDoS Mitigation System
4	Hardware Security	HSM Tampering Detection System
5	Security in Futuristic Technologies	Lightweight Post Quantum Messaging
6	Cryptography	Privacy Preserving KYC Verification System
7	Security in distributed wireless networks (IoT/CPS, 5G, etc.)	Wireless Protocol Fuzzing
8	Cyber Forensics	AI-based Log Investigation Framework
9	Governance, Operations & Privacy	Consent Management System
10	Fintech Security	Mule Accounts & Collusive Fraud in UPI

3. Stages

1. Ideation and Proposal Submission
2. Preliminary Evaluation and Shortlisting of Top 50 Ideas
3. Prototype Development and Evaluation (Top 50 Teams)
4. Mentorship, Capacity Building, and Prototype Enhancement (Top 20 Teams)
5. Final Evaluation of MVP and Winner Announcement (Top 3 Winners)

4. Prize Money

The students are eligible to win prizes up to Rs. 40 lakhs under various categories as listed below :

Category	Award	Amount (INR Lakh)	Amount (INR Lakh)
Final Winners	1st Prize	10	22
	2nd Prize	7	
	3rd Prize	5	
Special Recognition	Most Innovative Idea Award	3	8
	Women-in-Tech/Diversity Award	3	
	Jury's Choice Award	2	
Interim Support	Finalists (Top 20 Teams)	0.50	10
	Total		**40 akhs**

5. Eligibility Criteria

The Cyber Security Innovation Challenge 1.0 (CSIC1.0) is open to **student and researcher pursuing Bachelors, Masters and Doctoral studies from the academic ecosystem**. Applicants must be **below 30 years of age** at the time of application and should be citizen of India. The challenge welcomes student-led teams, researcher-led or researcher-assisted innovators, and student-led startups that aim to develop cyber security solutions aligned with India's critical sectors and emerging digital landscape.

Participants should demonstrate strong interest in cyber security innovation and commitment to progressing their ideas from concept to Minimum Viable Product (MVP) within the structured five-stage challenge framework, as per specified timelines.

6. Registration Fee

The Registration is free for all eligible participants.

7. How to Apply

Step 1: Visit the Official Website

Visit the official webpage for the Cyber Security Innovation Challenge 1.0 (CSIC 1.0)(https://www.dsci.in/content/cyber-security-innovation-challenge-10), which encompasses details on challenge domains, expected outcomes, rules and regulations, eligibility criteria, and stage-wise details.

Step 2: Click on "Apply Now"

On the landing page, click the **"Apply Now"** button. The candidate will be redirected to the ISEA Virtual Platform (IVP) for registrations.

- The candidate needs to create their login at IVP page using their email id
- Fill the required details along with the details of their team members.

Step 3: Prepare Your Submission

Create a document in **PDF format** and a **video** explaining the innovative cyber security idea against the chosen problem statement. Ensure that the submission highlights:

- Understanding of the real-world cyber security problem
- Proposed solution and technical approach
- System architecture
- Expected outcomes
- Benchmarking against existing solutions
- Differentiation and unique value proposition
- Product roadmap and end-use cases

The candidate needs to ensure that the idea is creative, feasible, impactful, and addresses a real cyber security challenge. Focus on the innovation, applicability, and scalability of the concept

Please note: ***Submissions must be entirely original, created solely by the participant, and not generated using any AI tools. Participants must ensure that their work does not infringe on any third-party intellectual property rights. The committee will conduct credibility and integrity checks to verify authenticity, and any submission found to contain plagiarized or AI-generated content will be disqualified immediately.***

Step 4: Upload Documents on the Portal

Submit the document in **PDF format** and **video** through the IVP platform, as per the instructions provided.

Step 5: Upload No Objection Certificate (NoC):

The team lead must upload a NoC from their institute stating:

- The student/team is permitted to participate in the competition.
- In case of MVP stage 3 funding, the funds will be transferred to the institution and disbursed in full without deductions to the student/team.

Step 6: Complete and Confirm Submission

- Review all details carefully and ensure that all required documents are uploaded.
- Submit the application through the portal and retain confirmation for future reference.

8. Details of Innovation Challenges Stages

The Cyber Security Innovation Challenge 1.0 features an innovative five-stage structure designed to guide innovators from the ideation phase to the development of a Minimum Viable Product (MVP). These stages include:

. Stage	Stage Description	Teams Remaining
Stage 1	Ideation and Proposal Submission	All Initial Entries
Stage 2	Preliminary Evaluation and Shortlisting of Top 50 Ideas	Top 50 Teams
Stage 3	Prototype Development and Evaluation of Top 50 Ideas	Top 20 Teams
Stage 4	Mentorship, Capacity Building, and Prototype Enhancement of Top 20 Ideas	Top 20 Teams
Stage 5	Final Evaluation of MVP and Winner Announcement of Top 20 Ideas	Top 3 Winners

8.1 Stage 1: Ideation and Proposal Submission

In stage 1, participating teams can apply for minimum 1 and maximum 5 listed problem statements on IVP platform and submit their innovative idea through a document in PDF format and a short video through the IVP portal. The proposal should articulate the problem understanding, proposed solution, technical approach, architecture, expected outcomes, benchmarking against existing solutions, and the unique value proposition along with the product roadmap.

This stage emphasizes creativity, feasibility, impact, and scalability of the idea. The team lead must also upload a No Objection Certificate (NoC) from the institute confirming participation approval and fund disbursement terms. This initial submission forms the foundation for evaluating the team's innovation potential and readiness for the subsequent stages.

8.2 Stage 2: Preliminary Evaluation & Shortlisting of Top 50 Ideas

In stage 2, submissions will be evaluated on the basis of eligibility, problem statement clarity, relevance to cyber security, and innovation quotient which will lead to shortlisting of top 50 teams. The evaluation criteria will be:

- **Technical Prototype Development (MVP 1) – 35%**
  - ✓ Functionality and innovation of the prototype.
  - ✓ Scalability and security robustness.
  - ✓ Quality of demo/working model.

- **Viable Product Roadmap & End Use Cases – 35%**
  - ✓ Practicality of deployment in real-world cyber security ecosystems.
  - ✓ Clear timeline for development and scaling.
  - ✓ Defined target market/user base.

- **Technical Clarity & Articulation – 30%**
  - ✓ Ability to explain architecture, security mechanisms, and implementation.
  - ✓ Depth of domain knowledge in domain applied.
  - ✓ Quality of pitch/presentation/documentation.

The results will be communicated to the shortlisted teams and also displayed in the CSIC webpage.

8.3 Stage 3: Prototype Development & Evaluation

In stage 3, top 50 teams will create a **Technical Prototype** under mentorship guidance along with structured feedback on participant engagement, roadmap viability, end-use cases, technical articulation and responsiveness.

Top 50 teams will showcase their technical prototype through demo videos/pitch decks (MVP 1) within specified timelines.

Evaluation Component: All the submitted prototypes will undergo a rigorous evaluation process by the jury (Industry+ Academia) and will be based on the scores awarded during evaluation.

- **Technical Maturity & Innovation (25–30%)**
  - ✓ Stability and completeness of the MVP (working solution, not just a demo).
  - ✓ Depth of cyber security innovation (use of AI/ML, blockchain, zero-trust, threat detection, etc.).
  - ✓ Security robustness and ability to withstand simulated attacks/penetration testing.
  - ✓ Compliance with security standards and best practices.

- **Scalability & Deployment Readiness: Relevance to current/future cyber security challenges (20%)**
  - ✓ Feasibility of scaling the solution for enterprise/large-scale use.
  - ✓ Infrastructure readiness (cloud-native, API integrations, interoperability).

- ✓ Performance testing metrics (speed, accuracy, reliability).
- ✓ Readiness for pilot deployment in industry/government environments.

- **Market Viability & End-Use Case Fit (20%)**
  - ✓ Clarity of problem-solution fit in cyber security ecosystem.
  - ✓ Market research: Who are the intended users (CISOs, SMBs, govt agencies, citizens)?
  - ✓ Clear business model & value proposition.
  - ✓ Competitive benchmarking: What makes this solution stand out?

- **Technical Clarity, Documentation & Articulation (10–15%)**
  - ✓ Quality of technical documentation, architecture diagrams, and process flow.
  - ✓ Ability of the team to articulate their approach to both technical and non-technical juries.
  - ✓ Clarity in communicating threat models, use cases, and technical differentiators.

- **Mentorship Engagement & Iteration (10–15%)**
  - ✓ How effectively the team has incorporated mentor's feedback from stage 3.
  - ✓ Evidence of iteration: Has the MVP significantly improved?
  - ✓ Willingness to adapt based on cyber security domain experts' advice.

- **Impact & Sustainability (10%)**
  - ✓ Long-term cyber security impact (policy relevance, social benefit, critical infrastructure protection).
  - ✓ Potential to create employment, startups, or collaborations in the ecosystem.
  - ✓ Sustainability: Roadmap for next 2–3 years (funding, go-to-market, partnerships).

At the end of stage 3; **top 20 teams will be shortlisted** based on the merit. Their solutions may cover some but not all of the 10 challenge themes. Results will be declared via email and on the official webpage.

8.4 Stage 4: Mentorship, Capacity Building, and Prototype Enhancement

In stage 4, top 20 finalists will be provided with:

- ✓ Expert-led webinars on technical topics, product development, pitching and some GTM Support.
- ✓ One-to-one mentorship sessions with industry leaders and cyber security professionals.

Each qualified team in top 20 will get INR 50,000 grant money for Prototype Enhancement.

Inclusions:

- ✓ The grant money will be directly disbursed to the institute after deducting the TDS.
- ✓ The institute will transfer the money to the team lead's bank account.
- ✓ The grant money may be used for purchase of hardware, software tools, cloud credits, test kits, security solutions, or licenses needed for advancing the MVP.
- ✓ Travel & logistics for attending workshops/ mentorship meetings and other operational expenses.

Exclusions:

- ✗ Day-to-day living costs, rent, food, entertainment, or personal gadgets not related to the challenge.
- ✗ Investments in stocks, crypto, mutual funds, or businesses unrelated to the innovation challenge.
- ✗ No lump sum distribution among team members without a plan for project-related utilization.

Expected Outcomes:

- ✓ Refine the submitted idea into a more tangible and implementable plan.
- ✓ Help finalists build a Minimum Viable Product (MVP).
- ✓ Improve technical and business aspects through feedback.

8.5 Stage 5: Final Evaluation of Minimum Viable Product MVP and Winner Announcement

In stage 5, top 20 finalists will be eligible for final MVP submission. Each finalist team will be required to submit a fully developed **Minimum Viable Product (MVP**) within the specified timelines, that demonstrates their complete solution. The submission must include:

- ✓ A working product or live demo showcasing end-to-end functionality.
- ✓ Comprehensive technical documentation, covering system architecture, cyber security mechanisms, implementation details, and identified use cases.
- ✓ A business model, deployment strategy, or adoption plan (where applicable) highlighting scalability, sustainability, and industry/government relevance.
- ✓ User experience and design elements (UI/UX) that improve usability and adoption potential.

The final submissions will undergo a rigorous, multi-dimensional evaluation conducted by a panel of distinguished experts from industry, academia, and government. The process will assess both the technical strength and the real-world applicability of the solutions. The jury will evaluate each product against the following dimensions:

- **Functional performance & reliability – 20%**
  - ✓ Assesses the consistency and promised delivery of the product.

✓ Evaluates correctness, stability, and dependability.

- **Technical depth & cyber security robustness (incl. scalability & resilience) – 20%**
  ✓ Captures core technical strength.
  ✓ Focuses on secure architecture, scalability, fault tolerance, and resilience against threats.

- **Innovation quotient & improvement since initial submission – 15%**
  ✓ Rewards originality, creative approaches, and significant progress made during the competition.
- **Impact potential (societal, industry, or national security relevance) – 20%**
  ✓ Measures the meaningfulness and wide-reaching aspect of the solution.
  ✓ Looks at relevance for broader adoption and contribution to national priorities.

- **UI/UX quality (usability & adaptability) – 10%**
  ✓ Evaluates user-centred design, ease of use, accessibility, and adaptability across contexts.

- **Team's ability to articulate & defend their solution (presentation & Q&A) – 15%**
  ✓ Judges clarity, persuasiveness, and the team's understanding of their product.
  ✓ Assesses team's effective communication of both technical and non-technical audiences.

8.6 Final Results & Winner Announcement:

- ✓ Based on cumulative scoring, the top 3 teams will be selected by the jury.
- ✓ Results will be announced at Grand Finale.
- ✓ Winner's names will also be showcased on the official challenge website, media channels, and partner platforms for broader outreach.
- ✓ Certificates, prize money, and potential incubation/mentorship opportunities may be awarded to top teams to support further development and real-world deployment of their solutions.

8.7 Innovation Challenge Outcome and Next Steps:

After the MVP development stage, teams will move into the next phase where they are supported in refining their solution and preparing it for real-world deployment.

The winning teams will be connected with key stakeholders across the cyber security ecosystem including industry partners, mentors, and potential adopters to facilitate validation, integration, and market readiness.

This stage also aims to guide promising teams toward building a sustainable cyber security start-up.

9. General Rules & Regulations

- ✓ The Challenge is open to student and researcher innovators from the academic ecosystem pursuing Bachelors, Masters and Doctoral studies. Applicants must be below 30 years of age at the time of application and should be citizen of India.
- ✓ Candidates can participate only as a team (minimum of 3 participants and maximum of 5 participants in each team).
- ✓ While applying as a team, the candidate must choose one team lead, responsible for handling the communication and submissions.
- ✓ All communications will be made to the team lead at registered email id only.
- ✓ One team can apply for more than 1 problem statement and up to 5 problem statements.
- ✓ The idea and proposal must be original. The teams must avoid using AI tools to generate the submission. The committee will run checks, and if any submission is found to be AI-generated or copied or plagiarism, the same will be disqualified immediately.
- ✓ The teams must ensure that their work does not infringe on any third-party intellectual property rights.
- ✓ Submissions must include:
    - Proposal in PDF format
    - Video explaining the idea
    - No Objection Certificate (NoC) from the respective institution.
    - ✓ NoC confirms that institute permission for candidates' participation in CSIC 1.0 and thereby acknowledges to pass on the received funding to the candidate without deductions.
- ✓ All submissions must be made as per the timelines / deadline. No submissions would be entertained beyond the deadlines.
- ✓ Ideas will be evaluated based on creativity, practicality, technical strength, innovation, and real-world impact. The decision of the jury will be final.
- ✓ Once shortlisted, candidate will be guided by mentors through the MVP development phase. The candidate is, therefore, advised to attend the sessions and remain consistent during the challenge.
- ✓ Grants (where applicable) will be released through the institute as mentioned in the NoC. Institute may be asked to provide Utilization Certificate for the money disbursed to the candidate through them.
- ✓ The grant must not be used for salaries or compensation for team members, nor for the purchase of any capital equipment such as laptops, mobiles, GPUs, or similar items.
- ✓ If any team wants to withdraw from the challenge, the team lead needs to inform the organizers.
- ✓ The organizing team may update guidelines, rules, SOPs / processes, from time to time, if needed. Participants will be informed and are advised to visit the official webpage for new updates.
- ✓ Candidate’s personal details will only be used for the challenge and will not be shared without candidate’s permission.

Need Help?

For queries, assistance, or clarification, please reach out at: **csic.support@dsci.in**

We wish you the very best as you begin your journey in the challenge.

Let the innovation begin!

Warm regards,

Organizing Team

Cyber Security Innovation Challenge 1.0

CYBER SECURITY INNOVATION CHALLENGE 1.0

Under the Aegis of ISEA Project, MeitY

Organised under Information Security Education and Awareness (ISEA) Project, an initiative of Ministry of Electronics and Information Technology (MeitY), aimed at developing skilled human resources for a safe, trusted, and secure cyber space.

Scan for Complete Details
Register at: www.innovation.isea.app/