इलेक्ट्रॉनिकी एवं सूचना प्रौद्योगिकी मंत्रालय
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
सत्यमेव जयते

सी-डैक CDAC

ADVERTISEMENT - 21-04-2026

INVITATION TO COLLEGES / TECHNICAL INSTITUTIONS

to Host the OS (BOSS) Bug Bounty — National Level 2026

36-Hour PAN India Simultaneous Cybersecurity Hackathon

1. About the Programme

C-DAC invites applications from engineering colleges, technical universities, and research institutions across India to serve as official Host Institutions for the OS (BOSS) Bug Bounty 2026 — India's first national-scale simultaneous cybersecurity hackathon focused on an indigenous operating system.

The event is conducted under the aegis of the Software Samprabhuta Mission (SSM) of MeitY, Government of India, and forms part of the formal Pre-Investment Activities of the SSM programme. Participating institutions will have the unique opportunity to partner with C-DAC in a nationally significant initiative to strengthen India's sovereign technology ecosystem.

2. Event Snapshot

Event Name	OS (BOSS) Bug Bounty — National Level 2026
Format	36-Hour Simultaneous Hackathon across PAN India
Theme	Cybersecurity Vulnerability Assessment of BOSS GNU/Linux OS
Programme	Software Samprabhuta Mission (SSM) — MeitY, Govt. of India
Implementing Agency	C-DAC Chennai
Reference No.	CDAC/BOSS-BB/2026
Participants (per Venue)	Minimum 300 (students, researchers, ethical hackers)
Regions Covered	North (Delhi-NCR) | South (Chennai) | East (Mumbai) | West (Kolkata) — simultaneous execution
Contact	ssm-bugbounty@cdac.in

3. Regions Covered

The PAN-India regions—North, South, East, and West—are identified for hosting the BOSS Bug Bounty. The preferred cities are listed below, and institutions located within these cities are expected to apply.

Region	Target Cities
South	Chennai
North	Delhi NCR
East	Kolkata
West	Mumbai

4. Eligibility Criteria for Host Institutions

Applications are invited from institutions of the above-mentioned cities that meet the following minimum eligibility criteria:

- Registered engineering college, technical university, or research institution (AICTE / UGC / deemed university or equivalent).
- Located within or accessible from a major city, with good connectivity from a railway / bus hub (≤ 20 km).
- Possession of IT and networking infrastructure capable of supporting a 36-hour cybersecurity event (see Technical Requirements in Section 5).
- Minimum 200 computing stations (laptops / desktops) available for participant use.
- Ability to provide 24×7 operations including food, rest, power, and security for the full event duration.
- Demonstrated experience in hosting hackathons, technical fests, or large-scale academic events.
- Willingness to sign a Memorandum of Understanding (MoU) with C-DAC and comply with the BOSS Bug Bounty Rules of Engagement.

5. Technical Requirements

The following technical infrastructure must be available or provisioned by the Host Institution for the event:

IT & Network Infrastructure

- High-speed internet connectivity of 1 Gbps or above (dedicated bandwidth during event).
- Redundant ISP connection or backup internet connectivity.
- Enterprise-grade Wi-Fi coverage across all event venues.
- VLAN / network segmentation capability to isolate participant traffic.
- Capability to enforce internet restrictions (jammers or network controls) during specific event phases.

Cyber Range / Lab Capability

- Isolated testing environment with a minimum of 200 laptops / desktops for participants.
- IT experts on-site to assist with environment recreation and vulnerability simulation.
- Pre-configured vulnerable application setup (minimum 5 target applications) as provided by C-DAC.
- Logging and monitoring systems for event security and participant activity tracking.

Power & Physical Infrastructure

- 24×7 uninterrupted power supply with generator backup for the full 36-hour duration.
- UPS for critical infrastructure (servers, network equipment, judging stations).
- Adequate seating, desks, and charging points for all participants and volunteers.

Participant Facilities

- Continuous food and refreshments throughout the 36-hour event.

- Designated rest / sleeping areas for participants during the event.
- Sufficient washroom and hygiene facilities for the expected number of participants.

Event Management & Support

- A dedicated event coordination team of minimum 5 members from the institution.
- A minimum of 40 trained volunteers for an event with 300 participants (scaled proportionally for larger events).
- AV setup including stage, microphone system, and display screens for opening and closing ceremonies.

Accommodation & Logistics

- Availability of accommodation within 10 km of the venue, or preferably on-campus stay facility.
- Transport / shuttle support for outstation participants and jury members.

Security & Compliance

- Ability to enforce Rules of Engagement, Non-Disclosure Agreements, and C-DAC's security protocols.
- Readiness for NDA / legal compliance documentation with all participants.
- Safe and isolated testing environment controls to prevent spill over outside the designated cyber range.

6. Evaluation & Selection Process

Host Institutions will be evaluated by a C-DAC Jury Panel using a structured evaluation framework across 10 sections for a maximum score of 100 marks (with up to 5 bonus marks for advanced capabilities). The selection will be based on an on-site or virtual assessment conducted after receipt of applications.

Evaluation Summary (Max: 105 Marks)

- IT & Network Infrastructure [CRITICAL] — 20 marks (mandatory minimum: 12/20)
- Cyber Range / Lab Capability — 15 marks
- Venue & Accessibility — 15 marks
- Power & Physical Infrastructure — 10 marks
- Participant Facilities — 10 marks
- Event Management Capability — 10 marks
- Security & Compliance Readiness — 5 marks
- Accommodation & Logistics — 5 marks
- Outreach & Ecosystem Support — 5 marks
- Experience in Hackathons / Cyber Events — 5 marks
- Bonus: Cybersecurity Lab, CERT-In/CDAC Tie-Ups, Incubation — up to 5 bonus marks

Selection:

The institutes across the 4 regions with the highest score will be selected to host the BOSS Bug Bounty event.

7. Application Process

Interested institutions are requested to submit their application along with the following documents:

- Duly filled Host Institution Application Form (Annexure-1 to be sent to email: ssm-bugbounty@cdac.in).

- The email submissions can be of up to 35 MB in a single email; if the file size exceeds 35 MB, it may be submitted across multiple emails.
- Institutional profile highlighting relevant infrastructure, prior hackathon / event experience, and cybersecurity-related activities.
- Letter of intent from the Head of Institution confirming willingness to host the event and comply with C-DAC's requirements.
- Infrastructure capability declaration (IT, power, facilities) duly signed by the IT Head / System Administrator.
- Photographs / documentation of existing computing labs, network infrastructure, and event management facilities.
- The evaluation will be conducted based on the checklist provided in Annexure-2 for reference.

Application Submission	ssm-bugbounty@cdac.in
Subject Line	BOSS Bug Bounty 2026 — Host Institution Application — [Region] — [Institution Name]
Last Date for Application	05.05.2026
Site Evaluation (Jury Visit)	Will be intimated later
For Enquiries & Clarifications	ssm-bugbounty@cdac.in

8. Terms & Conditions

- C-DAC's decision on selection of Host Institutions is final and binding.
- C-DAC reserves the right to accept or reject any application without assigning reasons.
- Selected institutions will be issued a Letter of Confirmation / Work order by C-DAC prior to the event.
- All event-related expenses for venue setup, participant facilities, and logistics shall be as per the agreed terms in the Letter of Confirmation / Work order
- The event is subject to the Software Samprabhuta Mission programme calendar and may be rescheduled at C-DAC's discretion.
- Participating institutions agree to abide by all BOSS Bug Bounty Rules of Engagement and responsible disclosure policies.
- Selected venues must be able to accommodate a minimum of 300 participants simultaneously.

9. Financial & Payment Terms

C-DAC will compensate the selected Host Institution for hosting the BOSS OS Bug Bounty 2026 on a fixed-cost basis as detailed below. The payment structure is designed to ensure delivery quality and mutual accountability.

Engagement Type	Fixed-Cost basis
Fixed Cost per Venue	**Rs. 5,00,000/- (Rupees Five Lakhs Only)**
Event Duration	3 Days (including pre-event setup, 36-hour hackathon, and post-event data backup & closure)
Advance Payment	30% for pre-event activities

	70% of payment on successful completion of the Bug Bounty event, subject to C-DAC verification
Mode of Payment	NEFT / RTGS / Account Transfer

10. Payment Conditions & Obligations

- The fixed cost of Rs. 5,00,000/- (Rupees Five Lakhs Only) covers all venue-related hosting obligations for the full 3-day event period including pre-event setup (Day 1), the 36-hour Bug Bounty hackathon (Days 1–2), and post-event data backup and system closure activities (Day 3).
- 30% Payment will be released for the pre-event activities and 70% payment only upon successful completion of the Bug Bounty event as determined by C-DAC, and upon receipt of the following: (a) Completion Certificate signed by the Institution Head; (b) C-DAC-verified data backup confirmation; and (c) Signed declaration of complete data deletion from all participant machines.
- All participant machines (laptops / desktops) used during the event must be pre-installed with the BOSS GNU/Linux OS image as supplied by C-DAC. No other operating system, dual-boot, or alternate boot media shall be permitted on participant machines during the event.
- All event data — including participant findings, bug reports, system logs, vulnerability submissions, and any data generated during the hackathon — must be securely backed up and transmitted to C-DAC's designated secure server prior to event close. C-DAC will provide the secure data transfer protocol and credentials.
- Upon successful data backup and C-DAC acknowledgement, all local copies of event data must be completely and permanently deleted from all participant machines, institutional servers, and any storage media used during the event. The Host Institution must provide a signed Data Deletion Certificate to C-DAC within 24 hours of event conclusion.
- The fixed cost is inclusive of all hosting obligations. No additional charges, claims, or reimbursements will be entertained beyond the agreed fixed amount of Rs. 5,00,000/- per venue.
- Failure to comply with data backup and deletion obligations, or any breach of the Host Institution Agreement, may result in withholding or recovery of the payment at C-DAC's discretion.

11. About BOSS GNU/Linux

BOSS (Bharat Operating System Solutions) GNU/Linux is an Indian distribution of the GNU/Linux Operating System developed by C-DAC. It is the widely deployed indigenous OS in Indian government systems and the official reference platform for the SSM Sovereign OS development programme. BOSS OS supports all 22 languages in the 8th Schedule of the Indian Constitution and is designed to meet the interoperability, security, and accessibility requirements of Indian government digital services.

Annexure -1

HOST INSTITUTION APPLICATION FORM

OS (BOSS) Bug Bounty — National Level 2026

36-Hour PAN India Simultaneous Cybersecurity Hackathon

Instructions to Applicants

1. Fill all fields in capital letters unless stated otherwise.
2. Attach supporting documents as specified in each section.
3. Incomplete or unsigned forms will not be considered.
4. Submit via email to: ssm-bugbounty@cdac.in
5. Subject Line: BOSS Bug Bounty 2026 — Host Institution Application — [Region] — [Institution Name]
6. Max attachment size: 35 MB per email. Split across multiple emails if required.

SECTION A — BASIC INSTITUTION DETAILS

Full Name of Institution	
Type of Institution	
Affiliated University / Board	*(if applicable)*
Year of Establishment	
AICTE / UGC / Deemed University Approval No.	
NAAC / NBA Accreditation (if any)	

Address & Location

Complete Postal Address	
City / District	
State / UT	
PIN Code	
Region Applied For (North / South / East / West)	
Distance from Nearest Railway Station (km)	
Distance from Nearest Bus Terminal (km)	
Google Maps / Location URL	

Primary Contact Details

Name of Head of Institution	
Designation of Head of Institution	
Official Email ID (Head of Institution)	
Mobile No. (Head of Institution)	
Name of Nodal Officer / Event Coordinator	
Designation of Nodal Officer	
Email ID (Nodal Officer)	
Mobile No. (Nodal Officer)	
Institution Website	

SECTION B — ELIGIBILITY DECLARATION

Tick (✓) all applicable boxes. Unticked mandatory criteria may lead to disqualification.

Mandatory Eligibility Criteria	
☐	**Registered engineering college / technical university / research institution (AICTE / UGC / Deemed University or equivalent).**
☐	**Located within or accessible from a major city, with good connectivity from a railway / bus hub (≤ 20 km).**
☐	**Minimum 200 computing stations (laptops / desktops) available for participant use.**
☐	**Capability to host 24×7 operations including food, rest, power, and security for full 36-hour duration.**
☐	**Demonstrated experience in hosting hackathons, technical fests, or large-scale academic events.**
☐	**High-speed internet connectivity of 1 Gbps or above (dedicated bandwidth) available or can be provisioned.**
☐	**Ability to accommodate a minimum of 300 participants simultaneously.**

SECTION C — IT & NETWORK INFRASTRUCTURE [CRITICAL]

This section is marked CRITICAL. A score below 12/20 in the evaluation may disqualify the institution.

Available Internet Bandwidth (Mbps / Gbps)	
Is the bandwidth dedicated / unshared during events?	☐ Yes ☐ No
Redundant ISP / backup internet available?	☐ Yes ☐ No
Name of ISP(s)	
Enterprise-grade Wi-Fi covering all event areas?	☐ Yes ☐ No
Wi-Fi Technology Standard (e.g., Wi-Fi 6 / 802.11ac)	
VLAN / network segmentation capability available?	☐ Yes ☐ No
Internet restriction / jamming capability during event phases?	☐ Yes ☐ No
Total Number of Computing Stations Available (Laptops + Desktops)	
Approximate number of servers available on-site	
Logging & monitoring systems in place?	☐ Yes ☐ No

Additional Information / Remarks (IT Infrastructure):

SECTION D — CYBER RANGE / LAB CAPABILITY

Isolated testing lab / cyber range available?	☐ Yes ☐ No
Lab Name (if any)	
Total Seats in Isolated Lab	
IT experts on-site for vulnerability recreation?	☐ Yes ☐ No
Number of IT Support Staff Available During Event	
Pre-configured vulnerable application setup possible?	☐ Yes ☐ No
Number of Target Applications That Can Be Configured	
Dedicated Cybersecurity Lab / Centre of Excellence on campus?	☐ Yes ☐ No
Name of Cybersecurity Lab / CoE (if applicable)	
Existing tie-ups with CERT-In / C-DAC / Industry Cybersecurity Bodies?	☐ Yes ☐ No

Details of Tie-Ups (Organisation Name, Nature of Partnership)	

SECTION E — POWER & PHYSICAL INFRASTRUCTURE

24×7 uninterrupted power supply available?	☐ Yes ☐ No
DG / Generator backup for full 36-hour duration?	☐ Yes ☐ No
Generator Capacity (KVA)	
UPS for critical infrastructure (servers, network, judging)?	☐ Yes ☐ No
UPS Backup Duration (Hours)	
Total Seating Capacity of Event Venue	
Adequate desks and charging points for all participants?	☐ Yes ☐ No
Total Area of Event Venue (sq. ft. / sq. m.)	

SECTION F — PARTICIPANT FACILITIES (36-Hour Event)

Continuous food & refreshments can be arranged throughout 36 hrs?	☐ Yes ☐ No
Designated rest / sleeping area available?	☐ Yes ☐ No
Rest Area Capacity (No. of Persons)	
Adequate washrooms / hygiene facilities on-site?	☐ Yes ☐ No
Number of Washrooms / Restrooms Available	
Medical / First-Aid facility available on-site?	☐ Yes ☐ No

SECTION G — EVENT MANAGEMENT CAPABILITY

Number of Dedicated Event Coordination Staff Available	
Number of Trained Volunteers Available	
AV Setup available (Stage, Microphone, Display Screens)?	☐ Yes ☐ No
Maximum Participant Capacity for Simultaneous Seating	
Incubation / Innovation Ecosystem available on campus?	☐ Yes ☐ No

Social Media reach / promotion capability?	☐ Yes ☐ No
Social Media Handles (Twitter / LinkedIn / Instagram)	
Approximate Student Community Reachable for Promotion	

SECTION H — ACCOMMODATION & LOGISTICS

On-campus accommodation / hostel available?	☐ Yes ☐ No
On-campus Accommodation Capacity (No. of Persons)	
Hotels / Guest Houses available within 10 km of venue?	☐ Yes ☐ No
Name of Nearby Hotel(s) / Distance from Venue	
Transport / shuttle support available for participants & jury?	☐ Yes ☐ No
Nearest Airport & Distance (km)	
Nearest Railway Station & Distance (km)	

SECTION I — SECURITY & COMPLIANCE READINESS

Ability to enforce Rules of Engagement & C-DAC security protocols?	☐ Yes ☐ No
Readiness to execute NDA / legal agreements with all participants?	☐ Yes ☐ No
Safe & isolated testing environment controls available?	☐ Yes ☐ No
Security personnel available for 36-hour coverage?	☐ Yes ☐ No
Number of Security Personnel Available	
CCTV surveillance across event area?	☐ Yes ☐ No
Institution willing to pre-install BOSS GNU/Linux OS on all participant machines?	☐ Yes ☐ No
Institution agrees to data backup & deletion obligations as per C-DAC requirements?	☐ Yes ☐ No

SECTION J — HACKATHON & CYBER EVENT EXPERIENCE

Number of Hackathons / Cyber Events Hosted (select one)	
☐	**0 – 1 events**
☐	**2 – 3 events**
☐	**4 – 6 events**
☐	**7 – 10 events**
☐	**More than 10 events (national / international preferred)**

List of Major Hackathons / Cyber Events Hosted (Last 5 Years):

S.No.	Event Name	Year	No. of Participants	Organiser / Sponsoring Body
1				
2				
3				
4				
5				

SECTION K — DOCUMENT CHECKLIST

Tick (✓) each document enclosed. Incomplete submissions will not be processed.

Documents to be Submitted Along with This Form	
☐	**Duly filled Host Institution Application Form (this form) — signed by Head of Institution.**
☐	**Institutional Profile — highlighting relevant infrastructure, event experience, and cybersecurity activities.**
☐	**Letter of Intent from the Head of Institution — confirming willingness to host and compliance with C-DAC requirements.**
☐	**Infrastructure Capability Declaration — IT, power, facilities — signed by IT Head / System Administrator.**
☐	**Photographs / documentation of computing labs, network infrastructure, and event management facilities.**
☐	**Copy of AICTE / UGC / Deemed University Approval Certificate.**

☐	**Details of existing MoUs with government bodies / industry partners (if applicable).**
☐	**Previous event report / brochures of hackathons hosted (if applicable).**

SECTION L — DECLARATION & SIGNATURES

Declaration

We, the undersigned, hereby declare that:

1. All information furnished in this application form is true, correct, and complete to the best of our knowledge.
2. We understand that submission of false or misleading information will result in automatic disqualification.
3. We agree to abide by all terms, conditions, and Rules of Engagement as stipulated by C-DAC for the BOSS Bug Bounty 2026.
4. We are willing to sign a Memorandum of Understanding (MoU) with C-DAC upon selection.
5. We confirm our ability to pre-install BOSS GNU/Linux OS on all participant machines and comply with data backup and deletion obligations.
6. We accept that C-DAC's decision regarding selection of Host Institutions is final and binding.

Nodal Officer / Event Coordinator	**Head of Institution (with Official Seal)**
Name: _____	Name: _____
Designation: _____	Designation: _____
Signature: _____	Signature: _____
Date: _____	Date: _____
	Official Seal / Stamp:

FOR C-DAC OFFICE USE ONLY

Application Reference No.: CDAC/BOSS-BB/2026/APP-_____

Date of Receipt: _____ Received by: _____

Acknowledgement sent on: _____ Mode: ☐ Email ☐ Portal

Site Evaluation Scheduled: _____ Jury Member: _____

Final Score: _____ / 105 Status: ☐ Selected ☐ Waitlisted ☐ Rejected

Remarks: _____

Annexure 2

HOST INSTITUTION EVALUATION CHECKLIST

OS (BOSS) Bug Bounty — National Level 2026 | 36-Hour PAN India Simultaneous Cybersecurity Hackathon

Institution Details

Institution Name	
Region	
City / State	

Scoring Guide

Instructions

- Enter only whole numbers within the maximum for each criterion.
- Section subtotals are auto-bounded by the maximum marks for that section.
- IT & Network Infrastructure is marked CRITICAL — a score below 12/20 in this section may disqualify the institution regardless of total score.
- Bonus marks (up to 5) are awarded over 100 for advanced capabilities.

Section 1: Venue & Accessibility (Max: 15 marks)

No.	Evaluation Criterion	Max Marks	Score Awarded
1.1	Within city limits / non-remote location	5	
1.2	Distance ≤ 20 km from Railway / Bus hub	5	
1.3	Internal campus accessibility & navigation	5	
Section Total		**15**	

Remarks / Observations:

_____

Section 2: IT & Network Infrastructure [CRITICAL] (Max: 20 marks)

No.	Evaluation Criterion	Max Marks	Score Awarded
2.1	High-speed internet (≥ 1 Gbps dedicated bandwidth)	4	
2.2	Redundant ISP / backup connectivity	4	
2.3	Enterprise Wi-Fi coverage across all event areas	4	
2.4	Internet restriction capability (jammers / network controls)	4	

2.5	VLAN / network segregation capability	4	
Section Total		**20**	

Remarks / Observations:

_____

_____

Section 3: Cyber Range / Lab Capability (Max: 15 marks)			
No.	**Evaluation Criterion**	**Max Marks**	**Score Awarded**
3.1	Isolated testing environment available (min. 200 laptops / desktops)	5	
3.2	IT experts on-site to recreate vulnerabilities / pre-configured vulnerable applications (min. 5)	5	
3.3	Logging & monitoring systems in place	5	
Section Total		**15**	

Remarks / Observations:

_____

Section 4: Power & Physical Infrastructure (Max: 10 marks)			
No.	**Evaluation Criterion**	**Max Marks**	**Score Awarded**
4.1	24×7 power with generator backup for full event duration	4	
4.2	UPS / uninterrupted supply for critical infrastructure	3	
4.3	Adequate seating, desks, and charging points for all participants	3	
Section Total		**10**	

Remarks / Observations:

_____

Section 5: Participant Facilities for 36 Hours (Max: 10 marks)			
No.	**Evaluation Criterion**	**Max Marks**	**Score Awarded**
5.1	Continuous food & refreshments throughout the event	4	
5.2	Designated rest / sleeping arrangements for participants	3	
5.3	Washrooms & hygiene facilities adequate for participant count	3	
Section Total		**10**	

Remarks / Observations:

_____

Section 6: Event Management Capability (Max: 10 marks)			
No.	**Evaluation Criterion**	**Max Marks**	**Score Awarded**
6.1	Dedicated event coordination team (minimum 5 members)	4	
6.2	Volunteers — ≥ 40 for 300 participants (scaled proportionally)	3	
6.3	AV setup: stage, microphone system, and display screens	3	
Section Total		**10**	
Remarks / Observations: _____			

Section 7: Security & Compliance Readiness (Max: 5 marks)			
No.	**Evaluation Criterion**	**Max Marks**	**Score Awarded**
7.1	Ability to enforce Rules of Engagement and C-DAC security protocols	2	
7.2	NDA / legal compliance readiness (participant agreements)	2	
7.3	Safe testing environment controls to prevent external spill over	1	
Section Total		**5**	
Remarks / Observations: _____			

Section 8: Accommodation & Logistics (Max: 5 marks)			
No.	**Evaluation Criterion**	**Max Marks**	**Score Awarded**
8.1	Nearby accommodation available (≤ 10 km from venue)	2	
8.2	On-campus stay facility (preferred)	2	
8.3	Transport / shuttle support for outstation participants & jury	1	
Section Total		**5**	
Remarks / Observations: _____ ___			

Section 9: Outreach & Ecosystem Support (Max: 5 marks)			
No.	**Evaluation Criterion**	**Max Marks**	**Score Awarded**
9.1	Promotion capability — reach to students, startups, cyber community	2	
9.2	Industry / Startup ecosystem linkages	2	
9.3	Branding & social media support for national promotion	1	
Section Total		**5**	
Remarks / Observations:			

Section 10: Experience in Hackathons / Cyber Events (Max: 5 marks)		
Select (✓)	**Hackathon Experience Band**	**Marks**
☐	0 – 1 events	1
☐	2 – 3 events	2
☐	4 – 6 events	3
☐	7 – 10 events	4
☐	More than 10 events (national / international preferred)	5
Remarks / Observations:		

BONUS: Advanced Capabilities (+5 marks over 100)			
No.	**Evaluation Criterion**	**Max Marks**	**Score Awarded**
B.1	Dedicated Cybersecurity Lab / Centre of Excellence on campus	2	
B.2	Existing tie-ups with CERT-In / C-DAC / industry cybersecurity bodies	2	
B.3	Incubation / innovation ecosystem for startups and tech initiatives	1	
Section Total		**5**	
Remarks / Observations:			

Final Score Summary

Section	Max Marks	Score Awarded
1. Venue & Accessibility	15	
2. IT & Network Infrastructure [CRITICAL]	20	
3. Cyber Range / Lab Capability	15	
4. Power & Physical Infrastructure	10	
5. Participant Facilities (36 hrs)	10	
6. Event Management Capability	10	
7. Security & Compliance Readiness	5	
8. Accommodation & Logistics	5	
9. Outreach & Ecosystem Support	5	
10. Experience in Hackathons / Cyber Events	5	
Bonus: Advanced Capabilities	5	
GRAND TOTAL (excluding bonus)	**100**	
GRAND TOTAL (with bonus)	**105**	

Selection:

The institutes with the highest score will be selected to host the BOSS Bug Bounty event.