CENTRE FOR RAILWAY INFORMATION SYSTEMS (CRIS) as part of ‘Content Delivery Network,Bot Detection Tools and Solutions to prevent content Scrapping’ is interested in pre-feasibility knowledge gathering exercise for the implementation of solution/s through an open Expression of Interest. Interested system integrator may visit website www.cris.org.in for further details or contact PPE/I&S, CRIS, Chanakyapuri, Near Bihar Niwas, New Delhi-110002, Phone: 011- 24104525 Ext 341 or emailat crisappsec@cris.org.in. The last date of submission of proposal is 03/03/2025 (17:00 hrs.).

Indian Railways

CENTRE FOR RAILWAY INFORMATION SYSTEMS

EXPRESSION OF INTEREST

FOR

CDN, BOT DETECTION & CONTENT SCRAPPING SOLUTIONS

New Delhi

Table of Contents

1. **EOI Schedule and Address**

S.No	Events	DateandTime
1	Brief Meeting on Expression of Interest (EOI) Document	**24.02.2025,10:30Hrs**
2	Last Date and Time for completed EOI document submission	**03.03.2025;17:00 hrs**
3	Address for EOI submission and all communication on the subject (IR/CRISAddress)	**GM/Infra** **CRIS,Chanakyapuri,NearBiharNiwas,NewDelhi-21**

** In case the designated dayhappens to be a holiday;the next working day will be deemed as the last date for submission of EOI.

Brie fMeeting on Expression of Interest(EOI) will be held on dated 24.02.2025 at CRIS Conference Hall 3rd Floor ITPI Building IP Estate New Delhi-110002

2. **Disclaimer**

2.1. This document is based on study of various literatures/papers available worldwide, by CRIS. Although every care has been taken in specifying details appropriately and unambiguously, CRIS shall not be liable for any kind of damages/lossesincurredbyanyand/orallduetoerrorsoromissionsinthis document.

2.2. This document mentions numerous commercial and proprietary trade names, registered trademarks and the like (not necessarily marked as such), patents, production and manufacturing procedures, registered designs, and designations. CRIS points out very clearly that the present legal situation in respect of these names or designations or trademarks must be carefully examined before making any commercial use of the same. Names of industrially produced apparatus and equipment may be included to a necessarily restricted extent only and any exclusion of products not mentionedinthisdocumentdoesnotimplythatanysuchexclusionhasbeen based on quality criteria or any other qualifying consideration.

2.3. CRIS expressly states that CRIS/ IR shall not be held responsible for any lossofanysortrisingtoanyperson/bodyorpartyduetothisEoIorthe

Knowledge-gathering Exercise referred to in this document or for any claims arising therefrom and all such claims shall be summarily rejected.

2.4. IR/CRIS is not committed either contractually or in any other way to the applicantswhoseapplicationsare accepted.The issue ofthisRequestforEOI does not commit or otherwise oblige the IR/CRIS to proceed with any part or steps of the process.

2.5. Since this is not a Request for Proposal (RFP), commercials are not required to be submitted at this stage.

3. Copyright

3.1. CRIS asserts its copyright of this document. No part of this publication maybe reproduced in any form without the prior permission of CRIS.

3.2. Enquiries relating to the copyright of this document may be addressed to the General Manager/ Infra, CRIS, New Delhi

4. About CRIS: -

The Ministry of Railways established the Centre for Railway Information Systems (CRIS) in 1986 as the umbrella organization for all computerization activities on Indian Railways. CRIS is a project-oriented organization engaged in development of major computerized systems and applications on IR. CRIS has a pan-IR reach and a vastrolloutsupportcapability.Witharichpracticalexperience,itsdedicated teamof professionals and inhouse R&D, CRIS leads in technology driven business transformation initiatives for Indian Railways

5. Background

The Ministry of Railways has recently introduced the SuperApp 'SwaRail'—a transformative digital initiative designed to provide a seamless, user-friendly, and comprehensive railway service experience to the public. Developed by the Centre for Railway Information Systems (CRIS), this SuperApp consolidates major public-facing applications of Indian Railways into a single integrated platform. Currently in beta testing, the app is available for download on both Google Play Store and Apple App Store.

To ensure the highest levels of efficiency, security, and reliability, CRIS is seeking technology vendors and OEM partners who can contribute their expertise in the domains as specified in this document.

6. ObjectiveofExpressionofInterest:

6.1. Content Delivery Network (CDN):

6.1.1. Offload compute and processing of static content (e.g., images, .js, HTML, XSS, etc.).

6.1.2. Improve user experience and web application performance.

6.1.3. Reduce latency, distribute load efficiently, and achieve 100% availability and reliability of services.

6.2. Web Application & API Protection (WAAP) Solution:

6.2.1. Act as the first line of security on the internet.

6.2.2. Protect web applications against OWASP Top 10 threats, including SQL Injection, XSS, LFI/RFI, etc.

6.2.3. Provide DDoS protection to mitigate cyber threats before they reach the origin.

6.2.4. Implement origin cloaking to safeguard backend services.

6.3. Advanced BOT Solution:

6.3.1. Provide protection against sophisticated bot attacks, credential stuffing, and account takeover (ATO).

6.3.2. Incorporate behavioural anomaly detection to prevent web scraping and data theft.

6.3.3. Reduce bot-related server load, bandwidth consumption, and latency.

6.3.4. Secure both web and native mobile applications to ensure only legitimate users access the services.

6.4. Advanced API Security:

6.4.1. Deliver comprehensive API discovery, inventory management, and vulnerability detection.

6.4.2. Offer risk management solutions against OWASP Top 10 API threats, including BOLA and BOPLA, amongst others.

6.4.3. Enable proactive API threat detection and business logic attack prevention.

6.4.4. Ensure API compliance, security testing (shift-left), and data residency within Indian boundaries.

6.5. Authoritative DNS Solution:

6.5.1. Provide cloud-based authoritative DNS to ensure 100% availability of all DNS zones managed by CRIS.

6.5.2. Incorporate in-built DDoS protection and performance-based DNS solutions.

6.5.3. Support DNSSEC and offer DNS zone monitoring for brand and name abuse detection.

6.6. Managed Security Services:

6.6.1. Offer managed security services for WAAP, Advanced BOT Protection, and API Security.

6.6.2. Ensure solutions are correctly configured as per best security practices.

6.6.3. Provide support for security incident response, attack monitoring, and remediation.

6.7. Log Retention, Processing & Real-Time Observability Solution:

6.7.1. Ensure a 180-day log retention policy across all solutions.

6.7.2. Provide real-time visibility into all traffic and security events.

6.7.3. Offer compression, encryption, and secure processing of log data in compliance with regulatory requirements.

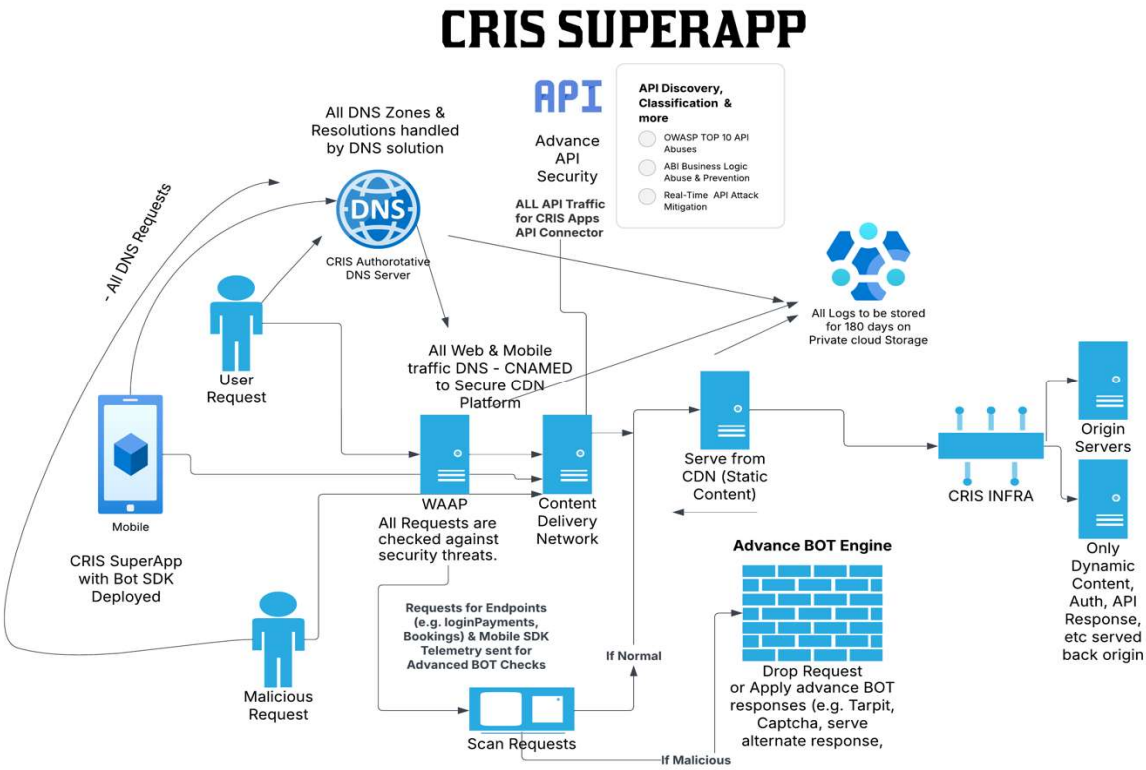
7. General Requirements:

- Services must be integrated to deliver comprehensive information from multiple sources in a unified manner.
- Ensure a 100% availability SLA across all proposed solutions.
- All data and critical services should adhere to security, privacy, and regulatory guidelines set by CRIS and the Ministry of Railways.

CRIS invites OEMs to submit their feedback and express their interest in participating in this initiative. Interested vendors are requested to provide a detailed response covering:

- Company profile and relevant experience.
- Proposed solution(s) and alignment with CRIS's requirements.
- Technical capabilities and compliance with security best practices.
- Support and service models.
- Indicative timelines for deployment and implementation.

8. High Level Draft Architecture



9. Invitation

Expression of Interest (EOI) is invited in a sealed envelope superscripted with "Expression of Interest (EOI) – Implementation of Bot Detection Solution and Solution to prevent Content Scrapping**" From the interested applicants / bidders.**

9.1. Who have solution strictlyin linewith the Broad Scope of Work as set out in this EOI and Agree to abide by the terms and conditions contained in this document.

9.2. Please note that the EOI is not a qualification criterion. IR/CRIS will float a separate RFP at its own discretion.

9.3. A Sealed envelope containing complete set of signed hard copy of EOI document and

delivered in person at the undernoted office (on any working day) on or before the date and time mentioned in "EOI Schedule and Address" section of this document

10. **Applicant's/Bidder'sEligibilityCriteria**

10.1. Bidder could be System Integrator (SI) partnering with OEMs of SOC technologies and front ending for the project or OEM who is also a system integrator,partneringwithotherSOCtechnologiesOEMsandfrontendingfor the entire project.

10.2. The bidder shall list out all prerequisite and proposed Security Solutions to achieve intended objective as specified in this document

11. **Payments/Guarantees/Insurancesetc.fortheexercises**:-

11.1. No payments shall be due to the System Integrator for this knowledge-gathering exercise.

11.2. There will be no charges to be paid by the SI to CRIS/ IR for these pre-feasibility knowledge-gathering exercises. The takeaway for IR would be exposure to various Deployment Architecture, Model (Cloud/Non-Cloud) technologies available in the area and their capabilities, Approach for Implementation of comprehensive Solutions to achieve intended objectives as specified in this document.

11.3. Participating in the pre-feasibility knowledge-gathering exercise does not confer anyrightstotheSI or the OEM oranyrelated agencyfor preference in award of any contracts in the future. It is reiterated that this is purely a knowledge gathering exercise mutually benefitting IR and the SI. This knowledge-gathering exercise also does not bind CRIS/ IR in any manner to limit its search for technology/ vendors/ SIs and or award of the final contract(s),ifandwhentheyareawardedatall,toanypartyotherthanthose that participate in this exercise.

12. ProcessbeforesubmissionofEOI

12.1. ModificationinRequestforEOIdocument:

12.1.1. At any time prior to the deadline for submission of EOI, CRIS/IR may modify any part of this document. Such change(s) if any may be in the form of an addendum /corrigendum and will be uploaded in IREPS/CRIS website at https://cris.org.in, ---→Tenders--→EOIforBotDetectionSol

12.1.2. All such change(s) will automatically become part of this EOI and binding on all applicants. Interested applicants are advised to regularly refer the IREPS/CRIS's URL referred above.

12.2. ExtensionofdateofsubmissionofEOI:

12.2.1. Request for extension of date for submission of EOI will not be entertained. However, the CRIS/IR at its discretion may extend the deadline in order to allow prospective applicants / bidder a reasonable time to take the amendment / changes, if any into account.

12.3. FormatandSigningofEOI

12.3.1. EOI should be submitted on A4 size paper, spirally and securely bound and

with all pages therein in serial order.

12.3.2. All EOI documents should be signed only by the authorized person(s) of the company/firm/bidder. Any interlineations, erases or overwriting shall be valid only if the person(s) signing the EOI authenticates them. The EOI should bear the rubberstampoftheapplicantoneachpageexceptfortheun-amendableprinted literature.

12.3.3. The applicants/ biddershoulddemonstrateorsubmittheirinputson compliance with Suggested eligibility criteria given in Annexure – 'A' of this EOI.

12.3.4. Asapart ofthisEOI,theapplicant hastosubmitdetailed approachpaperon how they propose setting up of desired Solution to meet the objectives defined in this document along withAnnexure-A,'B'andAnnexure-'C'tosetupthesame.

12.3.5. Power of Attorney should be submitted to support the authorized signatory status. Contact detail of the authorized signatory and an authorized contact person on behalf of the applicant is to be provided as under: -

Particulars	**Authorised Signatory for Signing the EOI**	**AuthorisedContactPerson**
Name		
Designation		
Email ID		
Landline		
Mobile No		
FaxNo.		
Address		

12.3.6. EOIshouldcomprise of

12.3.6.1. RequestforEOIdocumentdulysigned&stampedoneachpage

12.3.6.2. Your EOI in the proposed initiative along with documents / information / confirmation on the requirements as mentioned in this document with necessary supporting documents duly signed & stamped

12.3.6.3. Proposed solution document with suggested deployment architectureand related official supporting. It should includethe requirements / sizing on deployment

12.3.6.4. Completed EOI Documents along with Annexure-A, Annexure-'B' and Annexure – 'C' should be submitted in prescribed time line.

12.3.6.5. Submit compliance for Technical Specification as provided in Annexure-D. If Any change is required, Same can also be proposed along with detailed justification.

12.3.6.6. In case anydiscrepancy is observedbetween hard and soft copy,the hard copy will be considered as the base document.

13. HowtoParticipate

13.1. Pleasetakeaprintoutofthisdocument.

13.2. Collect/PrepareallthedocumentsasmentionedinthisEOIDocument- Ensure that all of these are complete.

13.3. The Authorized signatory must sign each page of the EoI document and anyother paper submitted in response to this EoI

13.4. Please submit all the documents in a closed cover so as to reach CRIS by the closing date. Please superscribe the envelope with "EOI FOR CDN Services along with Bot Detection and Content Scrapping Solution etc"

13.5. Theaddressis

GeneralManager(Infra)

CentreforRailwayInformationSystems

Chanakyapuri,NearBiharNiwas,NewDelhi– 1100021.

13.6. Foranyclarifications,pleasecontactatcrisappsec@cris.org.in

Annexure-A

S. No.	Parameter	Qualifyingcriteria	IndicateCompliancewith SuggestedQC
1.	CompanyExistence	shouldberegisteredfor morethan5yearsason date	Yes/No
2.	OEMor SI		
3.	Financial Turnover	Between Rs 150 Cr and Rs 225 Cr	
		BetweenRs2 2 5 Crand 300 Cr	
		More than 300Cr	
4.	Relevant Project/Work Experience of SOC	Single PO of Rs 66.37 Crfor Services specified in this document	
		Two contracts with similar services* costing not less than the amount equal to Rs. 47.40 Cr. Each	
		Three contracts with similar services* costing not less than the amount equal to Rs. 37.92 Cr. Each	
5.	Declaration regarding banning/Suspension.	should not be currently Banned/Suspended with any Government of India Agency/PSUonthedate ofclosingofthe Tender.	
6	Productdeployment	No of Deployment of Each OfferedProductsinLast3 FinancialYear	
7	Experience in implementation of 3CDN,Bot Detection, Content Scrapping Solution etc as specified in this document for Organisation working under Governemnt of India/PSUs,Autonomous Body etc or Public listed	No of such implementation in last 3 Financial Year.	

	company having turnover of more than 500 Cr turnover. .		

Annexure-B

ContentofTechnicalSubmissionbybidder

S.No	
1	Detailed unified Solution architecture for size, complexity and geographic spread and growth of IR vetted by OEM/s together. Proposed Architecture should clearly Confirm the hosting location of offered Solutions.
2	Estimated Size/Network traffic. Explain the rational how it is arrived at. Sizing guidelines for next five years
3	Provide a detailed functional architecture with data flow diagrams for the **CDN**, **Bot Detection**, **Content Scraping and other Solution as specified in this document**. Describe how data flows through the system, including interactions with web servers, bot detection engines, CDN edge nodes, and backend servers, as well as integration with SIEM for event correlation.
4	Describe the support mechanisms provided by **SI** and **OEMs** for **CDN**, **Bot Detection**, and **Content Scraping** tools in India. Include details of resource locations, availability, and the number of resources dedicated to supporting each OEM.
5	EachOEM'stechnology,innovationandfunctionalityroadmapoftheir product for first 3 years.
6	Provide a list of clients where the **SI** has successfully implemented **CDN**, **Bot Detection**, and **Content Scraping** technologies over the last three years. Specify the other technologies used and their relevance to the proposed solutions.
7	The project plan with high level description of project phases and estimated duration.
8	Compliance with MII Guidelines and Guidelines for Cyber Security Productsas issued by MeITY

9	Strategies in ensuring 100% uptime for Services being asked in this document.

	Notification dt.02.07.2018wasfurther revisedbyMeitY vide NotificationNo. 1(10)/2017-CLES dt.06.12.2019. Since the items (SIEM and EPP) in the subject tender are Cyber Security Products as per Annexure-I of MeitY's Notification dt.06.12.2019, MeitY's Notifications regarding Public Procurement (Preference to Make in India) for Cyber Security Products mentioned above are applicable against the subject tender, alongwith subsequent amendments, ifany.

Annexure-C

Details ofCompleteSolution Stack

S.No	NameofSolution	OEMMake/Model	MeITY Empanelled Public Cloud

Annexure-D

Draft Technical Specification for Solutions identified in this document

	Technical Specifications	
Section A	**Cloud Based Authorotative DNS Solution**	**Compliance Y/N**
1	The proposed solution must be fully cloud based Authoritative DNS solution providing low latency, reliable and secure DNS communication.	
2	DNS Platform should be purpose-built exclusively to serve DNS traffic to avoid any inter-dependency on other solutions on the provider's platform. DNS Platform to have multiple POPs globally andin india as well.	
3	Segmented Architecture design to handle both Performance and Availability aspects seperately to ensure there are no performance lag or possibility of a DNS system failure.	
4	DNS Platform should offer 100% Availability SLA, considering how important DNS availability is to Organisation in ensuring availability of critical services being provided by CRIS.	
5	The solution must be built on global anycast technology	
6	The solution must support low latency response time for DNS queries	
7	Authoritative DNS services should be ISO 27001:2013 & ISO 27701:2019 compliant	
8	Solution should support both primary and secondary DNS deployments	

9	DNS Service must support following Record Types: 1) A IPv4 Address 2) AAAA IPv6 Address 3) AFSDB AFS Database 4) CNAME Canonical Name 5) DNSKEY DNS Key 6) DS Delegation Signer 7) HINFO System Information 8) LOC Location 9) MX Mail Exchange 10) NS Name Server 11) NSEC3 Next-Secure, Version 3 12) NSEC3PARAM NSEC3 Parameters 13) PTR Pointer 14) RP Responsible Person 15) RRSIG DNSSEC Signature 16) SPF Sender Policy Framework 17) SRV Service Locator 18) TXT Text	
10	The DNS platform should be designed to avoid the known vulnerabilities and weaknesses associated with BIND architecture. The platform shall incorporate advanced security features at the non-BIND architectural level while still maintaining full compliance with DNS RFCs and IETF specifications.	
11	The DNS solution must support DNSSEC capability to secure DNS zones and records	
12	DNS service must provide protection against DDoS attacks directed at Centre For Railway Information Systems (CRIS)'s DNS Infra on their platform.	
13	DDOS Protection for DNS Solution should be bundled as part of the overall solution & there should be no seperate or extra fees for handling DDOS attacks. Centre For Railway Information Systems (CRIS) must not be billed for any Volumetric Attack Traffic at DNS Layer.	
14	If there is any DNS or DDOS attack on DNS Service, service provider should have neccessary detection & mitigation mechanism to ensure 100% Availability and no disruption to bank services.	

15	DNS service must provide DNSSEC with 'Sign & Serve' option. DNS Service provider must handle Key Rotation for DNSSEC and Centre For Railway Information Systems (CRIS) team should be offloaded of the task of Key Rotation. DNSSEC is required to protect Centre For Railway Information Systems (CRIS)'s DNS Infrastructure for emerging DNS based threats and DNS Service Provider should handle complete DNSSEC related key management and offer the same as a service to Centre For Railway Information Systems (CRIS).	
16	Solution Should offer protection for DNS attacks, such as DNS Security – DDoS DNS attack protection UDP/TCP/ICMP Flood DNS hijacking DNS amplification DNS reflection DNS Cache poisoning DNS NxDomain Attack	
17	The solution must have comprehensive volumetric DNS DDoS Protection with minimum 1 Tbps mitigation capacity	
18	The solution must allow users to create policy rules to block DNS resolution based on geographic location or IP prefix	
19	Rate-Limiting for DDOS to drop even a single IP should be available as part of the solution.	
20	During DDOS, DNS Security solution should have capabilities to apply positive security model and restrict DNS requests to a list of known-good DNS resolvers only.	
21	The solution must provide a management console (GUI) for managing DNS records	
22	The solution must also provide API for creating, modifying, and deleting DNS records	
23	The solution must provide Role Based Access Control (RBAC)	
24	The solution must enforce Two Factor Authentication for registered users	
25	Centre For Railway Information Systems (CRIS) must get Web Portal based access for configuration of DNS service	
26	Centre For Railway Information Systems (CRIS) must get facility to whitelist Centre For Railway Information Systems (CRIS) IP Addresses to Management Web Portal. This is to ensure that any configuration changes are done from Centre For Railway Information Systems (CRIS) network only	

27	Centre For Railway Information Systems (CRIS) must get facility to enable 2FA for Management Web Portal. This will provide additional layer of security for Centre For Railway Information Systems (CRIS) from configuration and reporting perspective	
28	DNS Service provider should provide unified portal to monitor complete DNS security related tasks like configuration, reporting, billing etc	
29	DNS Service Provider OEM must have their own First Party NOC, SOC, and Technical Support Centre (24 x 7 x 365) in India. This is to ensure that DNS Service provider has significant commitment towards India region. Centre For Railway Information Systems (CRIS) may request to visit these centres for verification of support & services centres.	
30	The solution must come with 24x7 OEM Support for break and fix issues	
31	The solution must show uptime status on GUI and must send monthly uptime reporting via email.	
32	The service shall have 24x7 Service hour support for 365 days and a ticketing mechanism to support time bound escalation and resolution support.	
33	Provide one-time detailed Training to Centre For Railway Information Systems (CRIS) technical team to manage the solution effectively	
34	Pricing for DNS must not be dynamic or traffic consumption based e.g. Based on DNS queries or traffic served. There should not be any extra cost to absorb DDoS attack traffic handled by the DNS platform for Centre For Railway Information Systems (CRIS) DNS Zones. Pricing should be predictable & Flat based on the number of DNS zones configurations as per Centre For Railway Information Systems (CRIS)'s requirement.	
35	DNS Solution should have security feature to Monitor and Protect DNS Zones & Brand	
36	Solution shold help identify for Phishing attempts & Domains used for a phishing campaign or for fake websites.	
37	Solution shold help identify Typosquatting. Domains that are a common misspelling or mistype of domain or brand.	
38	Solution should also present a Detailed DNS Security Report on domains that pose a threat to . Information should include risk indicators, URLs where the domain was used, Tags, WHOIS Registration Time when phishing domain was registered, and related threat information.	
39	Solution DNS Security Report should also include the number of threats based on the detected risk level and priority level.	

Section B	Secure CDN and Web Application & API Protection (WAAP)	Compliance Y/N
1	Secure CDN to act as the primary caching layer for to offload origin servers with any static content we want to cache. WAAP Solution to become the Primary layer of defence against cyber attacks such as Layer 7 attacks, DDOS, Bot and basic API attacks.	
2	Proposed Secure CDN solution shall have presence in: • Minimum 3,000+ PoPs globally with atleast 250+ PoPs in India • Globally Deployed across 100+ countries with strategic placement near ISPs and end-users. • Tier-1 Network Backbone: High-speed private backbone interconnecting key data centers. • At least 48 geographical locations across India and peering with all major Indian telecom service providers. • Traffic Delivery should only happen from india servers connecting to Centre For Railway Information Systems (CRIS) origin servers	
3	Proposed CDN solution shall support all key performance enhancing features, including • Caching of static content like JS, CSS, Images as well as Dynamic contents. • Caching of static content like JS, CSS, Images as well as Dynamic contents. • Caching of contents with configurable 'Time To Live' values. • Optimization techniques to accelerate content delivery and avoid Internet congestion points. • Shall support end users connecting over IPv4 & IPv6 from day one. • Shall be able to compress contents like Text, JS, CSS etc. on the last mile. • Shall identify the fastest, most reliable path to origin i.e. /Centre For Railway Information Systems (CRIS) Data Centers to retrieve and deliver dynamic/interactive content. • Shall provide following optimizations to improve performance: a. Object Pre fetching. b. Persistent Connections. c. Connection Pooling. d. Scalable TCP Window.	
4	The CDN Service Provider shall ensure that the proposed solution/platform shall has 100% uptime.	

5	The content delivered through the CDN services shall not degrade the performance of the origin website or content in any manner, even if the number of hits on the website increases exponentially.	
6	The CDN service shall support all prevalent types of desktop and mobile devices.	
7	The CDN solution shall have capability to support minimum 1 Million HTTP request/sec.	
8	The CDN solution shall have capability to support at least 15 Gbps Traffic Handling Capacity/Bandwidth.	
9	The CDN solution shall support country wise Geo Fencing/ Geo Restriction.	
10	The CDN solution shall have capability of mitigation against volumetric attack on Network Layer 3,4,7 etc., e.g. , TCP state exhaustion attacks, HTTP and UDP flood attacks, Reflective amplification attacks etc.	
11	The CDN solution shall support for minimum 100 TLS/SSL certificates.	
12	The CDN solution shall provide real time monitoring. The view shall be customizable. There shall not be any restrictions of number of users and concurrent logins to the monitoring dashboard.	
13	The bidder shall provide a security UI Dashboard for analysis purpose that contains upto 30 days of data. Bidder should also archive upto 180 days of logs/data. Also help in analysis if needed.	
14	The CDN solution shall provide white-listing as well black-listing of IPs/ IP range with up-to 50,000 CIDR list.	
15	The CDN solution shall provide implementation of ‘End To End’ TLS/SSL for HTTPS Traffic with TLSv1.2 & TLSv1.3.	
16	The CDN solution shall be capable of handling HTTP1.0, HTTP1.1, HTTP/2 and HTTP/3.	
17	The CDN solution shall be capable of conversion/transformation of Client’s HTTP versions into desired HTTP version while communicating with origin.	
18	The CDN solution shall provide a mechanism to test the rules/ configuration before going into production using a staging environment.	
19	The CDN solution shall have their own or 3rd party integration with threat-intelligence platform to protect against threats like botnet, C&C servers, malware domains, proxy networks, malicious IP addresses, hosts etc. For blocking as per advisory of Cert-IN/NCIIPC.	

20	The CDN solution shall have threat intelligence based on IP reputation and shall detect & block as well as log the traffic based on: a. Anonymous Proxies b. TOR IP Addresses c. Phishing Proxies d. Scanners e. Botnets f. Malicious IP Addresses g. Network used by Cloud Service Providers (CSPs) h. IP Reputation	
21	For effective dynamic caching, CDN should seamlessly facilitate the caching of APIs, optimizing their reuse to enhance overall offload performance.	
22	WAAP of CDN solution shall support both a positive security model and a negative security model. A negative security model explicitly defines known attack signatures. The negative security model shall include a pre-configured comprehensive and accurate list of attack signatures and Web application firewall shall allow signatures to be modified by the administrator.	
23	WAAP component of the CDN solution shall provide Web Application Filter for latest “OWASP Top 10 protection”	
24	WAAP of CDN solution shall provide application Layer Protection from prevalent common attacks.	
25	WAAP of CDN solution shall support AJAX/JSON application security for interactive web 2.0 based applications.	
26	WAAP of CDN solution shall be able to block invalidated requests as well as Tarpit the same if required.	
27	WAAP of CDN solution shall be able to block attacks before it is posted to the protected website/application.	
28	WAAP of CDN solution shall be capable to detect and mitigate application layer DDoS attacks like HTTP floods or DNS query floods by base-lining traffic.	
29	WAAP of CDN solution shall support creation of custom response against blocked attacks/ traffic.	
30	WAAP of CDN solution shall support rate limit based policies to control application layer attacks.	
31	WAAP of CDN solution shall be able to set a limitsw.r.t. URL length, request length, query string length, POST data length etc.	
32	WAAP of CDN solution shall be capable to configure list of allowed URLs, Deny URLs and take action accordingly.	

33	WAAP of CDN solution shall be capable to configure action based on file type e.g. allowed file type, disallowed file type etc.	
34	WAAP of CDN solution shall be capable to check HTTP protocol compliance and block requests if any violation is detected against HTTP protocol compliance.	
35	WAAP of CDN solution shall be capable to configure action based on HTTP methods e.g. allowed HTTP methods and disallowed HTTP methods etc.	
36	WAAP of CDN solution shall be able to provide protection against evasion techniques.	
37	WAAP of CDN solution shall be able to close all the sessions of attacker IP once it is banned.	
38	WAAP of CDN solution shall be able to implement rule to limit the number of request based on HTTP methods (GET/POST etc) from single IP address for specific time window.	
39	For a robust security posture CDN, WAAP, and Bot Management solution should all operate in-line mode and seamlessly integrate through a unified edge based platform. No traffic for onboarded Applications & APIs should goto origin directly.	
Section C	**Advanced BOT Management Solution**	**Compliance Y/N**
1	Advanced BOT Management Solution should offer 100% Availability SLA.	
2	BOT Solution should not be disjointed or 3rd party. It should be integrated & available via same platform such as CDN, WAAP along with Advanced Bot Solution. All of them should work inline.	
3	BOT management Solution should have SDK to support Android and iOS Apps. SDK should be able to retrieve user telemetry and send it to Bot Solution for verification.	
4	Advance Web Scraping Bot Solution should stop persistent scrapers from stealing content that can be used for malicious purposes.	
5	Differentiation Between Humans and Bots: Evaluate user behaviors and interactions to accurately distinguish between legitimate users and sophisticated bots.	

6	Solution should be purpose-built & have Multi-Layered Bot Assessment Approach. a. Protocol-Level Assessment: Use fingerprinting to evaluate how a client establishes a connection with the server. b. Application-Level Assessment: Ensure the client can execute business logic written in JavaScript. c. User Interaction Metrics: Analyze standard peripheral interactions such as touch screens, keyboards, and mice to confirm human activity. d. Risk Classification: Implement a deterministic classification system (Low, Medium, High) based on request anomalies.	
7	The Web Scrapping Bot solution must effectively mitigate the following threats: a. Site Degradation: Prevent excessive automated requests that degrade site performance. b. Competitive Intelligence Scraping: Block unauthorized data extraction used for business espionage. c. Site Metric Pollution: Ensure analytics accuracy by filtering out non-human traffic.	
8	Advanced Bot Solution should have following options to tackel Human fraud vs frauds caused by Bots	
9	Real-Time Fraud Analysis: Analyzesbehavior in real time to identify subtle signs of fraudulent activity from account creation through login and beyond.	
10	Account Opening Abuse Mitigation: Detect and prevent the creation of fake accounts used for fraudulent activities such as exploiting promotions, SMS pumping, testing stolen credit card information, hoarding inventory, and more.	
11	Account Takeover (ATO) Protection: Secure customer accounts against imposters attempting unauthorized access to steal data, conduct fraudulent transactions, or drain accounts.	
12	Sophisticated Adversarial Bot Attack Defense: Prevent credential stuffing, inventory manipulation, and other automated attacks often associated with account opening abuse and ATO.	
13	Comprehensive Account Lifecycle Protection: Identify and analyze user risk at all stages, including account creation, login, password changes, account updates, and financial transactions.	
14	Real-Time User Session Risk Scoring: Assess risk and trust throughout the user session to determine if a request is from a legitimate user or an imposter.	

15	Email Address Intelligence: Analyze the syntax and abnormal use of email addresses to detect fraudulent patterns.	
16	Email Domain Intelligence: Evaluate activity patterns from individual email domains, including disposable email services and excessive domain use.	
17	User Behavioral Profiles: Construct behavioral profiles based on previous locations, networks, devices, IP addresses, and activity timestamps to recognize returning users.	
18	Population Profiles for Anomaly Detection: Aggregate user profiles into a broader dataset to compare behavioral variances across an organization's user base for anomaly detection.	
19	Proposed bot mitigation solution shall work in conjunction with other components of the proposed solution, to effectively prevent/ protect against common bots as well as against bots that attempt to evade detection	
20	Bot mitigation solution shall be easy to configure without requiring any changes in DNS.	
21	Bot mitigation solution shall provide traditional bot detection techniques e.g., static request analysis, signature based detection etc.	
22	BOT Management Solution should provide following High-Level categories of BOTs: • Solution Provider BOT Categories covering known self-declared BOTs. • Customer Defined BOT Category • Unknown BOTs Category	
23	BOT Management Solution should detect unknown BOTs using: • user behavior analysis, • browser fingerprinting, • automated browser detection, • HTTP anomaly detection, • high request rate • Cookie integrity check • Session validation • behavioral telemetry from both regular devices & mobile phones	

24	Bot Management Solution should provide a wide range of actions that can be applied to different types of bots, including: • Monitor, • Skip, • Crypto Challenge, • Deny • Custom Deny • Slow, • delay, • serve alternate, • Tarpit/Silent Drop, • Allow, • Ignore, • Conditional Actions.	
25	Bot Management Solution should provide capability to create custom bot signatures and categories to identify specific bots and assign different actions based on the URL or time of day etc.	
26	Bot mitigation solution shall support creation of custom workflows for bot traffic, like, diverting malicious traffic to a different URL endpoint.	
27	Bot mitigation solution shall be able to automatically apply mitigation features, like, rate limiting when anomalous attack patterns are detected in the traffic.	
28	Bot mitigation solution shall support various rule actions – allow, deny/block, rate-limit, Challenge etc.	
29	Bot mitigation solution shall provide dashboards for monitoring of bot traffic details, in-depth analysis of Bot, Transactional End Point Protection Report, etc	
30	BOT management Solution should have support for website, mobiles apps for native/flutter based Android and iOS Apps.	
31	BOT Management Solution should not require any Hardware/Appliance/Software deployment in on-premise Data Centre.	
32	Internet Edge based solution provider should assign Bot Score to requests initiated by Bots on Transactional End Points of ’s online ticketing portal.	
Section D	**Advanced API Security**	**Compliance Y/N**
1	All API traffic going through providers CDN, WAAP platform should be covered by the solution.	

2	Deployment Flexibility: Should ever needed, Solution should Support cloud-hosted, self-hosted, hybrid, and distributed deployments as required by . For this project deployment should be in a private Saas instance of the OEM within India only. No API data should go outside India.	
3	Pre-Built Connectors support should be provided: Support integration with other platforms (as maybe available with the OEM) for 3rd party integration. Third-Party API Integration: Support integration with WAFs, Load Balancers, and API Gateways for additional API security solutions.	
4	Comprehensive API Discovery: The solution must automatically discover all types of APIs, including HTTP, RESTful, GraphQL, SOAP, XML-RPC, JSON-RPC, and gRPC, across the entire environment. This should be for all north-south APIs flowing through CDN & WAAP Solution.	
5	Shadow and Rogue API Detection: Identify legacy, shadow, and rogue APIs not managed by existing API gateways to ensure complete visibility.	
6	API Inventory Management & Classification: Maintain a robust API inventory with flexible tagging and grouping based on business units, applications, and relevant categories.	
7	Sensitive Data Protection: Classify and monitor sensitive data, such as credit card details, phone numbers, and social security numbers, flowing through APIs.	
8	Compliance Monitoring: Ensure continuous API compliance with frameworks like PCI DSS, GDPR, HIPAA, and internal policies. This can be based on the rules configured on the API Security Platform.	
9	OWASP API Security Top 10: Analyze APIs for misconfigurations and vulnerabilities, including those listed in the OWASP API Security Top 10.	
10	Real-Time Threat Detection and Prevention: Utilize AI and machine learning to monitor API traffic in real-time, detecting data leakage, data tampering, policy violations, suspicious behavior, and API security attacks, with options for automated or manual remediation.	
11	API Security Testing Module: Integrate security testing into the CI/CD pipeline to identify and remediate vulnerabilities during the development lifecycle.	
12	Pre-defined and Custom Datatypes: The solution should support pre-defined data types (tags) and allow defining custom data types via regex based on Centre For Railway Information Systems (CRIS) requirements.	
13	API Security Incident Reporting: The solution should provide a detailed summary of incidents, including evidence, reasons for the trigger, and steps for resolution.	

14	API Security Enforcement: The solution should have the capability to block attackers via WAAP or through its own solution.	
15	Automated Remediation Workflows: Enable automated workflows to respond to API security incidents, integrating with ITSM tools like ServiceNow, Jira, and Azure DevOps.	
16	Traffic Audit Capabilities: Record, visualize, and analyze API traffic to manage risk exposure from suspicious users and unusual API behaviors.	
17	Advanced Anomaly Detection: Use AI/ML-based detection for business logic attacks and other sophisticated threats.	
18	Detailed API Data Classification: Support bifurcation between API requests and responses with datatype tags such as PII, PCI, Sensitive, and Credentials.	
19	API Ownership & Change Logs: Allow defining API owners manually or automatically, and track API changes such as new fields, headers, and authentication updates.	
20	API Attack Analysis: Provide attacker-related data, including IP reputation, country, ASN, and past attack history.	
21	API Metrics & Reporting: Provide insights on API requests per hour/week, error rates, and trends.	
22	Incident Ticketing: Automatically or manually open tickets in external systems (e.g., Jira, Syslog) for security incidents, audit logs, and new API detections.	
23	Reporting & Dashboards: Provide comprehensive reports and dashboards for security posture and compliance monitoring.	
Section E	**Managed Security Services - MSS**	**Compliance Y/N**
1	Monitoring, Detection and Mitigation services should be provided for Security Solutions such as WAAP & Bot Solution.	
2	OEM should provide Managed Security Services for and Support 24X7, including weekends.	
3	Managed Security Service should not be 3rd party, but only from OEM. Support should be provided from india.	
4	OEM to provide in-house team of experienced security experts to do Proactive monitoring of security Alerts & Attack Events.	
5	OEM should provide regularly security configurations updates to maintain the highest levels of protection in the the ever-changing threat landscape.	
6	Provide a Post-Event Report that includes in-depth, postmortem report highlighting the attack behaviours and actions taken following an attack or security incident	

7	Provide at least 2-4 Technical Security Review yearly including In-depth analysis of security solutions with tuning recommendations	
8	Provide a named & Aligned Security Expert to for High-level security engagement and expertise to manage our business & security priorities.	
9	Monthly Security Report: Provide summary of security activity, overall security posture and project updates	
10	Provide a Customer Business Reviews: Executive summary of 's security activity for a business quarter, value confirmation, industry trends, and product roadmap	
11	Should have at least three 24X7 SOC team locations globally, including 1 in India to ensure they have proper resource coverage and Business continuity plan in place.	
12	Centre For Railway Information Systems (CRIS) Teams should be provided Named Human Resources & comprehensive OEM Team throughout the project, including but not limited to: • Account Manager • Engagement Manager • Pre-Sales Engineer • Client Service Manager • Technical Project Managers • Solutions Architect • Security Consultants • Security Architects	
13	Support teams should include, but not limited to: • SOC Support - 24 X 7 X 365 - for Security Incidents • Technical Support (TAC) - 24 X 7 X 365 - For any Break-and-Fix & troubleshooting • NOC Support - 24 X 7 X 365 - if any underlining Platform Issues arises • Professional Services - India business days & Hours Dedicated Hotline to contact support should be provided. Response SLAs for critical situation, such as P1 should be assigned. Security experts to respond in less than 30 minutes.	
Section F	**Log Retention, Processing & Real-Time Observability Solution**	**Compliance Y/N**

1	Log Storage & Processing • For Authoritative DNS, CDN, WAAP, and Advanced Bot Solutions, All logs should be stored on cloud storage for 180 days. • Log data storage and processing should only occur within India.	
2	Observability & Data Processing • An observability solution should be implemented based on the logs generated for the above-mentioned solutions. • The solution should process and visualize data via a GUI Dashboard, such as Grafana (Open Source). • It should be capable of processing large volumes of log data and provide real-time/sub-second queries for troubleshooting.	
3	Log Optimization & Compression • High compression should be enabled to drastically reduce log size while ensuring no impact on query performance.	
4	GUI Dashboard Requirements • The dashboard should be customizable as per CRIS requirements. • It should support multiple data points on a single screen, covering all key parameters.	
5	Log Collection Methods. The solution should support the following log collection methods: • Batch Processing: JSON, CSV, and other character-delimited formats. • HTTP Streaming: JSON, CSV, and other character-delimited formats.	
6	Alerting & Monitoring • Alert Rules: Ability to create custom alert rules with queries and expressions to monitor specific metrics or log data. These rules should define thresholds that trigger alerts when breached. • Alert Instances: Each alert rule should generate multiple alert instances, enabling granular monitoring of different components or time series. • Flexible Notifications: Alerts should be sent through multiple channels, including email, Slack, PagerDuty, and webhooks. Users should be able to configure contact points for notifications. • Notification Policies: Should support hierarchical routing of alerts based on labels for efficient alert handling in large systems. • Silences & Mute Timings: Users should be able to temporarily pause notifications for specific alerts or time periods (e.g., during maintenance or off-hours).	
7	Performance & Query: The system should support a Peak Query Capacity of at least 100 queries per minute.	

8	Access Control: The solution should support up to 100 standard Grafana users with role-based access controls (RBAC).	
9	Security & Encryption between storage, processing engine and user • Communication should be enforced over TLS. • Token-based authentication should be used for securing access. • Non-secure port access should be disabled for ingestion, UI, and query endpoints.	
10	Data Encryption at Rest: • All CRIS Logs data should be encrypted at rest on the storage.	
Section G	**Security Dashboard**	**Compliance Y/N**
1	OEM should provide a unified and efficient dashboard to assess all security events across their products and capabilities, so that CRIS can take informed actions without needing to switch between multiple applications.	
2	For security troubleshooting – OEM's Security Dashboard should have mult-dimensional view to sort attacks by various parameters such as actions, countries, hostnames, URIs, Waf rules that can give granular visibility into the attack traffic.	
3	Security Dashboard should have option to review samples of offending traffic for deeper insights into the WAF Alerts and give accurate correlation to rules and explanation of why the traffic was caught by WAAP Solution.	
4	Security Dashboards should have Reports for Bots, Client reputation, Security trends, DDOS Trends & more.	
5	The proposed solution should provide historical data or reports for multiple timeframes i.e., hourly, daily, weekly, monthly, and customized period.	