सी-डॉट
C-DOT

Call for Partner Empanelment

Lead Generation Partners and Solution Partners for C-DOT Products/solutions

Domestic and International Markets

Document Particular	Details
Document Number	C-DOT/CfPE/Marketing/2026/1
Issuing Authority	Centre for Development of Telematics (C-DOT)
Date of Issue	02nd November 2026
Last Date and Time for Submission	01st December 2026
Submission Portal	https://mis.cdot.in/cdot_empanelment/login
Clarification Contact	partner.empanelment@cdot.in
Query submission deadline	23th November 2026

Abbreviations and Glossary

Term	Meaning
Applicant	An entity submitting an application under this Call for Partner Empanelment independently.
Lead Generation Partner	Lead Generation Partner shall be responsible for market development, customer access, opportunity creation and end-to-end deal support.
Solution Partner	Solution Partner shall be responsible for solution integration, implementation, commissioning, training and support.
C-DOT	Centre for Development of Telematics.
CAP	Common Alerting Protocol.
CBS	Cell Broadcast System / Solution.
CEIR	Central Equipment Identity Register.
CIOR	Centralised International Outroamer Register.
EWS	Early Warning System.
IMS	IP Multimedia Subsystem.
ISP	Internet Service Provider.
ITA	Internet Traffic Analyser.
MCX	Mission Critical Communications / Services.
NDA	Non-Disclosure Agreement.
NSA	Non-Standalone.
O&M	Operations and Maintenance.
PQC	Post-Quantum Cryptography.
PPDR	Public Protection and Disaster Relief.
PoC	Proof of Concept.
Portal	The online portal on which the Call for Partner Empanelment application shall be submitted by the applicant
Product	A grouped C-DOT offering for which a single product-

Term	Meaning
Category	category application is submitted under this Call for Partner Empanelment.
QKD	Quantum Key Distribution.
RAN	Radio Access Network.
RFP	Request for Proposal.
SA	Standalone.
SLA	Service Level Agreement.
Solution Partner	The Solution Partner shall be primarily responsible for solution design and sizing, third-party integration, project planning, installation, configuration, testing, commissioning, acceptance, documentation, training, O&M, first-line support, and billing collection.
TFM	Telecom Fraud Management.
TRINETRA	C-DOT’s enterprise cybersecurity platform.
Opportunity Approval	C-DOT’s written approval permitting a partner to pursue a defined product-country-customer opportunity subject to stated conditions.
Empanelment	Inclusion in a non-exclusive pool of qualified partners after completion of the applicable selection and onboarding processes.

Contents and Document Roadmap

Part	What the Applicant Will Find
Background	What C-DOT is; why the Call for Partner Empanelment is being issued; the two partner categories; the applicant journey; and how to use this document.
1. Scope of Work	Separate and common scopes of work for Lead Generation Partners and SIs, applicable across India and international markets.
2. Eligibility Criteria	Common pre-qualification, role-specific qualification and product-category-specific technical qualification criteria.
3. Products	Product Categories, their intended purpose and target users, and the annexures containing the corresponding concept notes.
4. Application Process	Step-by-step Call for Partner Empanelment submission process, followed by the process for empanelment and later opportunity/RFP stages.
5. Evaluation Criteria	Pre-qualification and technical evaluation criteria for evaluation of the Call for Partner Empanelment Applications.
Application Forms	One Common Application Form and separate forms for each Product-Category submitted on the portal.
Product Concept Notes	The concept notes for each product category, attached at the **Annexure J**.

Note: This Call for Partner Empanelment is the first stage of the partner-empanelment process. It is not itself an empanelment, award, customer mandate, territory allocation or commitment of business.

Background

About C-DOT

The Centre for Development of Telematics (C-DOT) is a premier telecommunications technology research and development centre based out of New Delhi, India. Established in 1984, C-DOT has played a significant role in the design and development of telecommunications technologies and solutions suited to India's communication requirements. Over the years, its technology portfolio has expanded from switching and fixed-line telecommunications systems to advanced solutions spanning mobile and broadband communications, network security, enterprise cybersecurity, telecom fraud prevention, digital intelligence, public warning and disaster management, mission-critical communications and quantum-secure communications.

C-DOT's mobile communications portfolio includes 4G/5G Core and Radio Access Network, IP Multimedia Subsystem and Private 5G solutions. Its cybersecurity and telecom-security portfolios include Enterprise Cybersecurity Platform, Telecom Fraud Management solutions, Central Equipment Identity Register, Centralised International Outroamer Register and Internet Traffic Analyser. The product "TRINETRA" has been developed as an integrated enterprise cybersecurity platform that brings together multiple security functions for monitoring, detection, analysis and response.

C-DOT has also developed solutions for public warning and disaster management, including the Common Alerting Protocol-based platform and Cell Broadcast Solution, as well as Mission Critical Communications and Public Protection and Disaster Relief solutions for authorised public-safety and emergency-response users. Its emerging-technology portfolio includes Quantum Key Distribution solutions, quantum communication sub-systems and Post-Quantum Cryptography solutions for secure communications and cryptographic migration.

Collectively, these solutions are relevant to a broad range of users, including telecom operators, internet service providers, government departments, regulators, public-safety and disaster-management agencies, strategic organisations, enterprises and critical-infrastructure operators. The products covered under this Call for Partner Empanelment have been organised into twelve product categories. Section 4 provides a high-level description of each product category.

Purpose of this Document

C-DOT intends to expand the market reach, commercialisation and implementation of its products across India and international markets. This requires capabilities, that complement C-DOT's product-development and technical expertise, including market intelligence, customer access, local regulatory understanding, opportunity identification and development, bid and contract support, solution integration, site and network readiness,

implementation, testing, commissioning, training, operations, maintenance, lifecycle support and support for collection of payments for due invoice(s)

Through this Call for Partner Empanelment, C-DOT seeks to identify organisations with the relevant experience, market access, technical capability, resources and delivery capacity that may subsequently be considered for empanelment under two categories, namely, Lead Generation Partner and Solution Partner. The indicative responsibilities of both are defined below:

Partner Category	Primary Role	Indicative Responsibility
Lead Generation Partner	Development of market and identification of business opportunities.	Market assessment, account mapping, introductions, opportunity registration, customer engagement, bid coordination, commercial support, local stakeholder liaison and support for collection of payments for due invoice(s). A certain percentage of sales will go to the partner as per the agreement.
Solution Partner	Lead generation and/or implementation of solutions.	The Solution Partner shall be primarily responsible for solution design and sizing, third-party integration, project planning, installation, configuration, testing, commissioning, acceptance, documentation, training, O&M, first-line support, as assigned and collection of payments for due invoice(s) including wherever there is a direct billing from C-DOT to the customer. Additionally, the Solution partner shall be eligible to perform Lead Generation Partner role. A certain percentage of sales will go to the partner as per the agreement

Note: The Partners do not make commitments on behalf of C-DOT or without prior approvals from C-DOT.

An applicant may seek qualification as either a Lead Generation Partner and/or a Solution Partner. Where an applicant qualifies for Lead Generation role their scope of work remains limited to deal creation and realization while the implementation of the project is then performed by a Solution

Partner as per C-DOT's discretion. Empanelment in Lead Generation role does not automatically confer qualification in the Solution Partner role but a qualification as a Solution Partner automatically makes the applicant eligible to conduct lead generation activities also.

Domestic and International Applicability

The Call for Partner Empanelment is intended for applicants from India and other jurisdictions, subject to the legal, security, ownership, export-control and contracting conditions approved by C-DOT. Applicants proposing to work in the international markets must lawfully demonstrate their right to work in the given jurisdiction, an understanding of applicable local requirements and a credible delivery or partner ecosystem. All applicants remain subject to applicable Indian requirements and the requirements of the customer jurisdiction.

Applicant Journey

Stage	Applicant Action	C-DOT / Process Outcome
1. Call for Partner Empanelment process	Understand products, partner roles, scope, criteria and evidence requirements. Applicant decides the product categories and partner role(s) for which it will apply.	Put the partner empanelment process in its website with a online portal where applicants can apply
2. Call for Partner Empanelment response	Submit onlineone Common Application Form and separate Product-Category Forms for each selected category.	Process response is logged and validated with online acknowledgement of submission.
3. Application evaluation	Provide clarifications, presentations or evidence if requested.	C-DOT qualifies the applicants for empanelment stage through a committee
4. Empanelment Process	Applicants who qualify the evaluation stage shall be informed about further process for empanelment.	Selected entities will be informed for empanelment snd signing of agreement.
5. Onboarding	Execute agreement/NDA and complete product and process onboarding.	Entity becomes an empanelled partner for stated products and roles.
6. Opportunity / RFP stage	Register or respond to opportunities and RFPs identified directly from the	C-DOT determines opportunity-specific participation, responsibilities,

Stage	Applicant Action	C-DOT / Process Outcome
	market or seeded by C-DOT.	commercial terms and finalizing the partner for the opportunity as per the terms in the agreement
7. Delivery and support	Perform the scope assigned under the opportunity/project agreement.	Performance is reviewed against project/sales outcomes on an annual basis.

How to Use this Document

Applicants should first read this Background in full. Section 1 defines the Scope of Work of the Lead Generation Partners and Solution Partners. Section 2 lists out the mandatory pre-qualification and technical qualification criteria for eligibility. Section 3 describes the product categories of C-DOT. Section 4 specifies the Call for Partner Empanelment application process and the later stages that may follow. Section 5 explains how applications will be evaluated. The Application Forms at the end are the prescribed response formats that will be available on the online portal for the applicants to fill.

Note: Nothing in this Call for Partner Empanelment document authorises an applicant to represent C-DOT, approach a customer in C-DOT's name, share non-public product material, quote pricing, conduct a PoC, submit a bid or commit C-DOT resources without written approvals and agreement. Such actions shall be a punishable offense and shall be taken up in the Commercial/ Civil Courts in the Republic of India and in accordance with the applicable law.

1. Scope of Work

This section defines a common scope for each partner category across all product categories. This scope of work is only indicative and shall not be limiting in nature. The actual work for any opportunity will be defined in terms of activities allocated in the applicable written approval, mutually signed agreement, RFP, statement of work, or purchase order issued at any later stage. Product-specific technical requirements will be derived from the product and market requirements and opportunity identification.

1.1 Common Scope of Work for Lead Generation Partners

- **Market assessment and prioritisation:** Assess target sectors, customer segments, policy and regulatory context, procurement routes, competition, local ecosystem, funding pathways and timing in India and proposed international markets.
- **Account and stakeholder mapping:** Identify relevant operators, internet service providers, government bodies, regulators, public-safety agencies, enterprises, strategic organisations, development-finance institutions and local partners, as applicable to the product.
- **Opportunity identification and registration:** Identify credible product-country-customer opportunities and submit complete, accurate information in the formats that shall be prescribed by C-DOT before any external activity in C-DOT's name.
- **Customer access and discovery:** Arrange approved meetings, support discovery, document customer needs, decision processes, procurement status, budget/funding context and expected schedule, and communicate these accurately between C-DOT and prospective buyer.
- **Positioning and communication:** Use only C-DOT-approved presentations, product claims, references and communication material; may localise the engagement approach without changing approved technical or commercial claims.
- **Demonstration and PoC coordination:** Coordinate demonstrations and PoCs, including customer objectives, local logistics, prerequisites, permissions, timelines and closure documentation. Technical execution will be led by the identified Solution Partner assigned in writing.
- **Bid and procurement support:** Track RFIs, EoIs, RFPs and other procurement instruments; support bid/no-bid assessment; prepare local-market, eligibility, compliance and administrative inputs; and coordinate submission requirements and client meetings.
- **Commercial and contracting support:** Provide market intelligence on taxes, duties, payment practices, local content, bid securities, contractual norms, currency and payment security; support negotiations without binding C-DOT or making any commitments in the name of C-DOT.
- **Local regulatory and compliance support:** Identify telecom, cybersecurity, data, public-safety, import/export, certification, licensing,

sanctions, anti-bribery, intermediary and local-agent requirements and obtain professional advice where required.

- **Partner ecosystem development:** Identify and disclose proposed local agents, distributors, subcontractors, or consultants. No such intermediary may be appointed for a C-DOT opportunity without prior written approval and due diligence.
- **Pipeline governance and reporting:** Maintain an auditable product-wise pipeline, report status and next steps, disclose competing interests and avoid duplicate or inaccurate opportunity claims.
- **Support until customer closure:** Remain engaged in the opportunity from opportunity qualification, bid, negotiation to contracting as assigned, including coordination of clarifications and customer references.
- **Post-award relationship support:** Support stakeholder communication, issue escalation, customer feedback and identification of follow-on requirements, without interfering with the assigned project governance.
- **International-market responsibilities:** Maintain lawful right to work in respective country/jurisdiction, local language and business capability where needed, awareness of sovereign and security sensitivities, and compliance with Indian and destination-country requirements.
- **Protection of C-DOT's interests:** Preserve confidentiality, intellectual property, brand integrity and accuracy of representation; immediately report conflicts, integrity concerns, unauthorised disclosures or reputational risks.
- **Payment/Collection:** Responsible for enabling the immediate payment for all invoices/advances by the customer for all invoices due.

1.2 Common Scope of Work for Solution Partners

The Solution Partner shall perform the wider scope of work of the Lead Generation Partner along with separate technical scope of work listed below:

- **Requirement validation and solution design:** Convert the approved customer requirement into a complete solution boundary, architecture, sizing basis, bill of materials, third-party dependency list and responsibility matrix.
- **Site, network and infrastructure assessment:** assess data-centre, cloud, radio, transport, fibre, power, rack, cooling, security, device, interface, capacity, redundancy and field requirements relevant to the product.
- **Project planning and mobilisation:** prepare project, resource, procurement, logistics, quality, risk, cybersecurity, testing, acceptance, training, support and transition plans.
- **Third-party procurement and integration:** source and integrate third-party components, licences, equipment, applications and services approved by C-DOT on case basis; remain responsible for compatibility and support obligations assigned.

- **Local approvals and compliance:** support licences, certifications, approvals, import/export formalities, site permissions, security clearances, labour and tax requirements assigned under the project.
- **Installation and configuration:** undertake receiving, inspection, secure storage, installation, configuration, custom integration and environment preparation in accordance with approved documentation.
- **Interoperability and migration:** integrate with customer and third-party systems, conduct interface validation, support data or service migration, prepare rollback arrangements and manage change windows.
- **Testing and acceptance:** prepare test cases and acceptance criteria, undertake factory/lab/site testing as applicable, manage defect logs, evidence completion and obtain formal acceptance.
- **Cybersecurity and data protection:** implement assigned access control, hardening, logging, vulnerability management, data handling, privacy, incident reporting, secure remote support and customer security requirements.
- **Documentation:** maintain approved design, configuration, interface, inventory, testing, as-built, standard operating procedure, incident and acceptance documentation.
- **Training and knowledge transfer:** train customer administrators, operators, field teams and helpdesk personnel; provide manuals, runbooks and practical handover appropriate to the assigned scope.
- **Operations, warranty and support:** provide first-line monitoring, helpdesk, field support, spares, preventive and corrective maintenance, incident triage, SLA reporting and escalation to C-DOT as agreed.
- **Programme governance:** provide a named project manager, technical lead and escalation structure; report schedules, milestones, risks, dependencies, changes, quality and commercial status.
- **Subcontractor management:** remain accountable for approved subcontractors and local delivery partners, including capability, security, performance, compliance and continuity.
- **International delivery:** provide credible in-country mobilisation, customs and logistics planning, local skills, time-zone coverage, language support, remote-access controls and continuity arrangements.
- **Transition and closure:** complete handover, data and asset return, knowledge transfer, open-issue closure, warranty transition, continuity support and secure destruction/return of confidential material.
- **Payments/Collections :** Responsible for ensuring payments to C-DOT for all due invoices where billing is due by the Solution Partner or the end customer in case C-DOT is billing directly

1.3 Product-Specific Scope Overlay

For each product category, the specific scope of work, especially the technical component, shall be identified and shared at the stage of deal implementation.

1.4 Responsibility and Approval Principles

- Empanelment and shortlisting are non-exclusive and do not guarantee work, territory, customer access or revenue.
- Each product-country-customer pursuit requires C-DOT’s prior written approval before external representation or commitment as per the agreement.
- The customer-facing and contracting structure will be decided separately for each opportunity.
- Commercial terms, pricing, licence, margins/fees, taxes, warranties, liabilities, SLAs and payment protection are outside this document purview and will be fixed in later stage of the empanelment process.
- No partner may subcontract a material obligation, appoint an intermediary or use C-DOT’s name or logo without prior written approval.
- All pre-existing C-DOT intellectual property remains with C-DOT. Any project-created intellectual property and licence rights brought in by the partner will be stated in the applicable agreement/project agreement.

2. Eligibility Criteria

Eligibility is assessed in three layers: common pre-qualification applicable to every applicant; role-specific pre-qualification for Lead Generation Partner and/or SI; and product-category technical qualification. Mandatory criteria are pass/fail. Only applicants passing the applicable mandatory criteria will proceed to technical scoring.

2.1 Common Pre-Qualification Criteria

Ref.	Criterion	Minimum Requirement	Evidence
PQ-1	Legal existence	The Applicant must be a duly incorporated or registered legal entity in India or abroad in its respective country such as a company incorporated under Companies Act 1956/2013, a Limited Liability partnership (LLP), a partnership firm registered under LLP Act 2008 and must be legally capable of contracting for the proposed work. Foreign entities must be legally registered in their respective countries and possess the legal capacity to enter into binding agreements under Indian law. Such entities shall comply with all applicable laws in India, including those relating to Intellectual Property Rights (IPR), data protection, export control, cybersecurity, and other applicable regulatory requirements. Foreign entities shall also comply with national security requirements, telecom security directives, and restrictions issued by the Government of India from	Certificate of incorporation/registration and constitutional documents.

Ref.	Criterion	Minimum Requirement	Evidence
		time to time.	
PQ-2	Operating history	The Applicant must have completed at least three (3) financial years of operations as on the closing date.	Registration documents and statutory filings.
PQ-3	Financial capacity	The Applicant must have an average annual turnover of at least INR 5 Cr if they are applying as a Lead Generation Partner and INR 250 Cr if they are applying as Solution Partner, during the latest three completed financial years and positive net worth at the end of last financial year (2025-26) or the end of respective last financial year. For foreign entities, the equivalent turnover in freely convertible foreign currency shall be considered at the exchange rate prevailing on the date of issuance of this Call for Partner Empanelment. The applicant shall submit audited financial statements/ certified financial statements or equivalent documents for the relevant financial years.	Audited financial statements and auditor/qualified accountant certificate.
PQ-4	Solvency	The Applicant must not be under insolvency, liquidation, winding-up or comparable proceedings that materially impair performance.	Authorised declaration and supporting evidence if requested.
PQ-5	Debarment and integrity	The Applicant must not currently be debarred or blacklisted from business by C-DOT, the Government of India, an Indian State	Prescribed declaration and disclosures.

Ref.	Criterion	Minimum Requirement	Evidence
		Government, a PSU, the applicant's home government or a multilateral institution; no material integrity matter must have been concealed.	
PQ-6	Tax and statutory compliance	The Applicant must have valid registrations required in the applicant's jurisdiction and for the proposed role. Indian and international applicants will provide equivalent documents as applicable.	A valid PAN and GST registration and/or similar and equivalent registrations applicable in their respective country/jurisdiction. Tax and statutory registrations.
PQ-9	Litigation and regulatory disclosure	The Applicant must provide disclosure of material litigation, regulatory actions, criminal proceedings or investigations relevant to capability or integrity.	Prescribed disclosure and explanatory note.
PQ-10	Authority Certificate	The Applicant shall submit a duly executed Authority Certificate confirming that the person signing and submitting the Application is legally authorised to act for and bind the Applicant in all matters relating to this Call for Partner Empanelment.	Board resolution, power of attorney or equivalent authority.
PQ-11	Confidentiality and verification	Acceptance of confidentiality, verification, due diligence and reference-check requirements.	Signed undertaking.
PQ-12	International applicability	Where international markets are proposed, ability to contract, export/import and perform in the proposed jurisdictions, subject to	Relevant registrations, local presence/partner evidence or mobilisation plan.

Ref.	Criterion	Minimum Requirement	Evidence
		approvals.	

2.2 Role-Specific Criteria

Role	Role-specific Requirement	Indicative Evidence
Lead Generation Partner	At least [2] completed market-development, business-development, channel, advisory, bid or customer-acquisition assignments in the ICT sector during the previous [2] years; and a product-market opportunity approach.	Contracts/certificates, client references, market plan, country presence, account ecosystem and named BD team.
Solution Partner	The Solution Partner shall fulfil the role-specific requirement of a Lead Generation Partner as well as that of the Solution Partner as given below: At least [2] completed technology implementation/ integration assignments in the relevant or directly comparable domain during the previous [2] years; qualified technical and project-management resources; and first-line support capability.	Contracts/certificates, acceptance evidence, architecture/implementation summaries, certifications, support and field footprint.

2.3 Product-Category-Specific Technical Criteria

No.	Product Category	Product-Category Specific Requirement	Evidence
1	Mobile Communications	Completed or ongoing assignments involving mobile core, IMS, RAN, telecom network integration, rollout or managed services; access to telecom architecture, integration and field resources.	Product-Category Form, relevant assignments, client evidence, and technical approach.
2	Private 5G	Completed or ongoing private mobile-network, enterprise wireless, campus network or IT/OT integration assignments; enterprise use-case and local deployment capability.	Product-Category Form, relevant assignments, client evidence, and technical approach.
3	Telecom Fraud Management	Completed or ongoing telecom fraud, revenue assurance, data analytics or operator workflow implementations; experience integrating telecom data sources.	Product-Category Form, relevant assignments, client evidence, and technical approach.
4	Enterprise Cybersecurity	Completed or ongoing cybersecurity platform, SOC, SIEM, EDR, SOAR or enterprise-security assignments; qualified cybersecurity personnel and applicable certifications.	Product-Category Form, relevant assignments, client evidence and technical approach.
5	Central Equipment Identity Register	Completed or ongoing telecom-regulatory, device-identity, operator-integration, registry or high-availability government platform assignments.	Product-Category Form, relevant assignments, client evidence and technical approach.
6	Centralised International Outroamer	Completed or ongoing roaming, telecom-data integration, operator	Product-Category Form, relevant assignments, client

No.	Product Category	Product-Category Specific Requirement	Evidence
	Register	analytics or secure multi-operator platform assignments, with strong data governance capability.	evidence and technical approach.
7	Internet Traffic Analyser	Completed or ongoing ISP, network monitoring, traffic analytics, DPI/metadata, performance or network-assurance assignments, subject to lawful-authority controls.	Product-Category Form, relevant assignments, client evidence and technical approach.
8	Quantum Communications: QKD and Sub-systems	Completed or ongoing QKD, optical communication, cryptography, secure-network or strategic deep-tech integration assignments; specialised technical resources.	Product-Category Form, relevant assignments, client evidence and technical approach.
9	Quantum Communications: PQC	Completed or ongoing cryptography, PKI, application security, protocol integration, crypto-agility or migration assignments; specialised security resources.	Product-Category Form, relevant assignments, client evidence and technical approach.
10	Disaster Management	Completed or ongoing public-warning, CAP, cell broadcast, disaster-management, telecom integration, GIS, command-and-control or government platform assignments.	Product-Category Form, relevant assignments, client evidence and technical approach.
11	Mission Critical Communications	Completed or ongoing mission-critical, PPDR, public-safety, emergency communication, dispatch, control-room or resilient field-network assignments.	Product-Category Form, relevant assignments, client evidence and technical approach.
12	Digital Intelligence	Completed or ongoing telecom intelligence, anti-	Product-Category Form, relevant

No.	Product Category	Product-Category Specific Requirement	Evidence
	Platform	fraud, citizen-safety, secure analytics, government digital platform or multi-stakeholder integration assignments.	assignments, client evidence and technical approach.

3. Products

C-DOT invites applications against the following twelve product categories. The descriptions are high-level and are intended to help applicants determine relevance. They are not technical specifications, warranties or commitments. A concept note for each product category has been attached at **Annexure J** and provides the approved product-level context available for this Call for Partner Empanelment.

3.1 Mobile Communications

Products included: 4G/5G NSA Core, 5G SA Core, IMS and 4G/5G RAN

A mobile-network portfolio covering packet core, standalone 5G core, multimedia service control and radio access. The portfolio is intended for telecom operator, network-modernisation and selected private or institutional deployments. Depending on the approved configuration, partners may be required to support network planning, interworking, migration, interoperability, OSS/BSS and transport integration, testing, rollout and operations.

3.2 Private 5G

Products included: Private mobile-network solution

A dedicated 5G network offering for controlled enterprise or campus connectivity. It can support industry, utilities, logistics, mines, campuses and other operational environments where coverage, device connectivity, security, local control, edge integration or service assurance are important. Partner work may include use-case discovery, spectrum and regulatory assessment, site design, enterprise IT/OT and application integration, deployment and managed support.

Note: Private enterprise or campus networks shall ordinarily be covered under the Private 5G category. The Mobile Communications category applies primarily to public telecom, operator and other deployments expressly approved by C-DOT.

3.3 Telecom Fraud Management

Products included: TFM / telecom fraud-management platform

A telecom-focused platform intended to help operators identify, analyse, investigate and manage suspicious usage patterns and fraud risks using relevant network and business data. Partner work may include data-source mapping, integration, fraud-use-case configuration, workflow design, validation, tuning, training and operations support.

3.4 Enterprise Cybersecurity

Products included: TRINETRA

An indigenously developed, integrated enterprise cybersecurity platform that supports centralised monitoring and response across multiple

cybersecurity domains. C-DOT describes TRINETRA as supporting capabilities across areas such as endpoint management and detection, security information and event management, orchestration and response, behaviour analytics, data-loss prevention and security audit/compliance. Modules may be positioned as an integrated platform or individually, subject to the approved offering.

3.5 Central Equipment Identity Register

Products included: CEIR

A centralised system for managing mobile-device identity information and enabling authorised action against devices reported lost, stolen, invalid or otherwise required to be controlled under the applicable national framework. Deployment ordinarily requires coordination with telecom operators, regulators and authorised government entities, with strong requirements for integration, governance, security, auditability and high availability.

3.6 Centralised International Outroamer Register

Products included: CIOR

A centralised solution intended to support authorised management and analysis of international outbound-roaming information across participating telecom networks. The exact use cases, interfaces, governance, data treatment and authorised users will be as specified in the approved concept note and applicable law. Partners may be required to coordinate operator integration, secure data exchange, analytics workflows, testing and support.

3.7 Internet Traffic Analyser

Products included: ITA for Internet Service Providers

A network-traffic visibility and analytics solution for authorised use by ISPs and other approved network operators. It may support traffic monitoring, operational analysis and anomaly identification, subject to the approved interfaces, lawful authority and privacy/security requirements. Partner work may include topology assessment, sizing, collection-point integration, dashboard configuration, validation and operational support.

3.8 Quantum Communications: QKD and Sub-systems

Products included: QKD solutions and quantum communication sub-systems

Solutions for quantum key distribution and associated sub-systems used in supported high-security communication environments. Partner responsibilities may include use-case qualification, fibre and topology assessment, site and physical-security readiness, optical/network integration, key-management and encryption-system integration,

interoperability testing, specialised training and maintenance. Only C-DOT-approved performance and security claims may be used.

3.9 Quantum Communications: PQC

Products included: Post-Quantum Cryptography solutions

Solutions supporting assessment and migration toward cryptographic mechanisms designed to address future quantum-computing risks. Partner work may include cryptographic discovery and inventory, dependency analysis, crypto-agility assessment, pilot planning, application or protocol integration, testing, rollback planning, documentation and phased migration support.

3.10 Disaster Management

Products included: EWS CAP and Cell Broadcast Solution

An integrated public-warning portfolio comprising a Common Alerting Protocol-based early-warning platform and cell-broadcast dissemination capabilities. The solutions support authorised creation, approval and dissemination of geographically targeted alerts through connected channels and mobile networks. Deployment requires multi-agency governance, operator integration, multilingual configuration, drills, training, security, redundancy and operational procedures.

3.11 Mission Critical Communications

Products included: MCX and PPDR

Mission-critical voice, video and data communications for authorised public-protection, emergency-response, defence, critical-infrastructure and field users. C-DOT's MCX client is described as standards-based and designed for prioritised real-time communications over supported LTE, 5G and Wi-Fi environments. Partner work may include operational workflow design, devices, dispatch and command-system integration, trials, configuration, training, acceptance and high-availability support.

3.12 Digital Intelligence Platform

Products included: Modules that aid prevention of frauds, including cyber frauds, declaring a number as risk for payments through financial risk indicator, stolen mobile tracing etc that make up the digital intelligence platform

The concept notes for all product categories are attached at **Annexure J**.

4. Application Process

4.1 Guidelines for response to this Call for Partner Empanelment and submission steps

This Call for Partner Empanelment is Step 1 of a staged process. It is intended to identify and evaluate interested applicants at the levels of partner and product categories. The further stages may be refined by C-DOT and will be governed by the documents issued for those stages. The applicants are requested to follow the below mentioned steps while preparing and submitting their responses to this Call for Partner Empanelment:

Step 1: The Call for Partner Empanelment proposal application should be submitted through the online portal on the link provided on the title page of this document. No email or hard-copy submissions shall be taken into consideration for evaluation. All annexures and any corrigenda shall be communicated from a notified C-DOT channel.

Step 2: Applicant must Register and login to the portal. Thoroughly read through the Background, product descriptions, scopes, eligibility requirements and evaluation methodology.

Step 3: Select one or more of the twelve product categories and select the role they wish to apply for: Lead Generation Partner or Solution Partner.

Step 4: Complete the relevant Common Application Form, authorization letter, declarations for debarment, blacklisting, insolvency, financial strength, and integrity along with the product-category specific applications forms. The product-selection matrix in the common application form must identify every product category and role applied for.

Step 5: Complete one separate Product-Category Form for each selected product category. A combined response covering multiple product categories will not be considered.

Step 6: Attach documentation proof to prove qualification in each criterion. The file name and page number of the proof should be clearly referred to in the common application form.

Step 7: Declarations and authorization letter must be completed, signed by competent authority, stamped and submitted on the letter head of the applicant’s organisation.

Step 8: Upload all relevant documents in the sequence prescribed on the portal and use the standard naming convention defined on the portal.

Step 9: Submit through the portal before the deadline and retain the acknowledgement.

Step 10: Monitor the portal for corrigenda, clarification requests, presentation/demonstration invitations and evaluation communications.

4.2 Required Submission

The Applicant shall submit the documents listed below through the application portal. Each document must be clearly named, indexed and cross-referenced in the Common Application Form or the applicable Product-Category Form filled on the portal. Where a document is not applicable, the Applicant shall state “Not Applicable” and provide a brief justification.

Criteria / Requirement	Documents / Evidence Required
1. Application submission and acceptance of Call for Partner Empanelment conditions	**Covering Letter**, given at **Annexure A,** on the Applicant’s letterhead confirming the partner role or roles applied for, acceptance of the Call for Partner Empanelment conditions, and correctness of the information submitted must be uploaded on the portal before filling in the Common Application Form.
2. Common Applicant information	The **Common Application Form**, format given in **Annexure B**, including company details, product category and role selection, common pre-qualification response, financial information, and international experience and presence details must be filled on the portal and respective proofs and supporting documents must be uploaded and referenced appropriately as defined in subsequent requirements.
3. Authority of the authorised signatory	**Board Resolution, Power of Attorney, Letter of Authorisation or equivalent legally valid document** along with the Authority Letter appended at **Annexure E** on Applicant’s letter head must be uploaded on the portal against the relevant company details.
4. Product-category-specific response	A separate **Product-Category Form,** format given in **Annexure C, for each product category applied for**, including the Applicant’s understanding of the assignment, market or implementation capability, proposed approach, relevant experience, country coverage, etc. must be filled on the portal.
5. Legal status and operating history	**Certificate of Incorporation or Registration** and applicable constitutional documents, such as the Memorandum and Articles of Association, partnership deed, LLP agreement or equivalent documents must be uploaded against the relevant field of the Common Application Form. Where the incorporation or registration documents do not establish the prescribed period of operations, the Applicant shall also submit **annual statutory filings, annual reports, corporate-registry extracts or equivalent evidence** covering the required period.
6. Tax and statutory compliance	Copies of **tax registration certificates, business or trade registrations and statutory registrations** applicable in the Applicant’s jurisdiction must be uploaded on the portal against the relevant field of the Common Application Form. Indian Applicants shall submit **PAN, GST registration and IEC**, where applicable.

Criteria / Requirement	Documents / Evidence Required
	International Applicants shall submit equivalent documents applicable in their jurisdiction.
7. Financial capacity	**Audited financial statements for the latest three completed financial years** (2023-24, 2024-25, 2025-26) and a certificate issued by the statutory auditor, chartered accountant, certified public accountant or equivalent authorised professional confirming: (i) annual turnover for each of the three years; (ii) average annual turnover; and (iii) net worth for the latest completed financial year (2025-26) must be uploaded on the portal against the relevant field of the Common Application Form and format mentioned in **Annexure F.**
8. Solvency and continuity of operations	Signed **declaration confirming that the Applicant is not under insolvency, liquidation, bankruptcy, winding-up or comparable proceedings** that may affect its ability to perform the proposed engagement must be uploaded on the portal against the relevant field of the Common Application Form and format mentioned in **Annexure I**.
9. Blacklisting and Debarment	Signed **declaration confirming that the Applicant is not debarred or blacklisted** from business by C-DOT, the Government of India, an Indian State Government, a PSU, the applicant's home government or a multilateral institution must be uploaded on the portal against the relevant field of the Common Application Form and format mentioned in **Annexure H**.
10. Integrity resolution	Signed **Integrity Certificate**, on Applicant's letter head, must be uploaded on the portal against the relevant field of the Common Application Form and format mentioned in **Annexure G**.
11. Relevant experience and comparable assignments	For each assignment submitted as proof of experience, any one or more of the following documents must be uploaded on the portal against the relevant field in the Project-Category specific forms: **project completion certificate, satisfactory-performance certificate, client experience certificate, work order, purchase order, letter of award, signed contract or agreement, commissioning certificate, acceptance certificate, go-live certificate, client reference letter or other verifiable client-issued or client-acknowledged document**.
12. Lead Generation Partner capability, where applicable	Relevant **business-development, market-development, channel-development, advisory, customer-acquisition or bid-support assignment evidence**; evidence of existing country or market presence; and the **product-market opportunity-development plan and twelve-month activity plan** must be submitted on the portal as part of the applicable Product-Category Form, format mentioned in **Annexure C**.
13. Market access and customer ecosystem for Lead	Any of the following documents, depending on availability: **details of completed assignments in the proposed market, office or branch registration documents, publicly verifiable**

Criteria / Requirement	Documents / Evidence Required
Generation Partner, where applicable	**customer engagements, client reference letters, channel appointments, distribution or representation authorisations, or other verifiable documents demonstrating access to the relevant sector and customer segments** must be uploaded on the portal against the relevant field in the Product Category form, format mentioned in **Annexure C**. Confidential customer information must not be submitted without the customer's authorisation.
14. Solution Partner capability, where applicable	Relevant **implementation and systems-integration assignment evidence**; technical project summaries; solution-design and implementation methodology; testing and acceptance approach; project-management and quality-assurance approach; and details of implementation, field-support and operational capabilities must be submitted through the portal against the applicable Product-Category Form, format mentioned in **Annexure C**.
15. Operations, helpdesk and support capability for Solution Partner, where applicable	**Description of existing helpdesk or support arrangements, field-service locations, escalation structure, technical-resource strength, incident-management process and SLA support model**, supported by relevant SLA-based project credentials, customer certificates, service-management certifications or other verifiable evidence, where available must be uploaded on the portal against the relevant field of the Product-Category Application Form, format mentioned in **Annexure C**.
16. Product-category-specific technical capability	Evidence specified for the selected product category, including **relevant completed assignments, product or technology credentials, technical project descriptions, applicable product or industry certifications, and details of available technical resources**. The evidence must be uploaded on the portal against the relevant field of the for every Product-Category Application Form, format mentioned in **Annexure C**.
17. Country or market presence and mobilisation capability, where applicable	If the applicant wishes to apply for areas where the Applicant does not have an **existing presence, office or branch registration documents, tax or business registrations, staffing details, local operations information or completed assignment evidence**, they must submit a **Country or Market Mobilisation Plan** covering the proposed establishment, staffing, mobilisation schedule, customer-engagement arrangements, regulatory approach and delivery or support model on the portal against the relevant field of the for every Product-Category Application Form, format mentioned in **Annexure C**.

4.3 Submission Conditions

Item	Requirement

Language	English. Supporting documents in another language must be accompanied by a certified or otherwise acceptable English translation.
Format	Signed and stamped PDFs for all declarations, certificates, letters, and supporting documents uploaded on the portal must be readable and in standard language
File naming	All files uploaded on the portal must be named as follows: [Applicant]_[Common or Product (Category Name)]_[Document Name].
Submission channel	Portal with its link as stated on the cover page of this document.
Deadline	Deadline as stated on the cover page of this document. Late applications shall not be considered.
Corrigenda	Applicants must keep a track on the portal for any updates, clarifications, or corrigendum shared by C-DOT. A corrigendum or any such documents prevails over inconsistent earlier text.
Clarifications	Questions must be submitted through the portal before the deadline mentioned on the cover page of this document. C-DOT may publish responses of general relevance without identifying the applicant.
One application	An applicant may submit only one application in the capacity permitted by the portal.
Costs	Each applicant bears its own costs of preparing and submitting the Call for Partner Empanelment and participating in evaluation.

4.4 Clarifications, Presentations and Due Diligence

C-DOT may seek written clarifications, request original or additional documents, contact customers and issuing authorities, invite presentations or demonstrations, conduct facility visits, and undertake legal, financial, technical, security, ownership and integrity due diligence. Clarification may explain or substantiate an existing submission but may not be used to create eligibility after the closing date, except where C-DOT applies a documented and consistent approach permitted by the process.

4.5 Evaluation Principles

- Evaluation will be performed for each applicant based on the submitted common application form and each selected product category and partner role.
- The common pre-qualification criteria (Section 2.1) is applicable to all applicants.
- The role-specific criteria (Section 2.2) is separately applicable for Lead Generation Partners and Solution Partners.
- The product-category-specific technical criteria is separately applicable for respective product category applied for
- Technical evaluation will be undertaken only for responsive applications as defined in Section 5.2 below.
- Claims without verifiable evidence shall receive no marks.
- C-DOT shall standardise scoring guidance before evaluation and use a multi-member committee to improve consistency.
- Empanelment shall be subject to due diligence, conflict review, competent-authority approval and execution of definitive documents.
- C-DOT may qualify multiple applicants for the same product and role. Ranking or qualification does not create an entitlement to work.

4.6 Evaluation Stages

Stage	Assessment	Evaluation Outcome
0	Responsiveness check: timely submission, product-role selection, required forms and evidence.	Responsive / non-responsive.
1	Common pre-qualification under Section 2.1.	Pass / fail at applicant level.
2	Role-specific criteria under Section 2.2.	Pass / fail for Lead Generation Partner and Solution Partner.
3	Product-category technical criteria under Section 2.3.	Pass / fail for each selected product category.
4	Technical scoring against the applicable role and product category.	Score out of 100 for each product-role combination.
5	Clarification, presentation, demonstration, reference check and due diligence, as required.	Validated score.
6	Evaluation committee recommendation and competent-	Selected / Waitlisted / Rejected.

Stage	Assessment	Evaluation Outcome
	authority decision.	
7	Subsequent call for empanelment and onboarding.	Empanelled status only after agreement execution and written confirmation.

4.7 Technical Evaluation: Lead Generation Partner

Criterion	Marks	Assessment Focus
Relevant sector and product-market experience	25	Experience in lead generation, business development, market development, channel development, strategic advisory, bid support, customer acquisition or market-entry assignments relevant to the selected product category. Evaluation will consider the relevance, scale, complexity, geography, applicant's actual role and demonstrated outcomes of completed assignments.
Market access and customer ecosystem	25	Demonstrated access to relevant customer segments, including telecom operators, internet service providers, government departments, regulators, public-safety agencies, critical-infrastructure operators, strategic organisations, enterprises and other potential customers applicable to the product category. Existing in-country presence, customer relationships, local partnerships and supporting evidence will also be considered.
Product-market opportunity development plan	20	Understanding of the selected C-DOT product category, target use cases, proposed markets, priority customer segments, procurement and funding routes, applicable regulatory environment, competitive landscape, opportunity-identification methodology and proposed activities for the first twelve months.
Proposed team and geographic coverage	15	Availability and suitability of the proposed business development team, including sector specialists, country or regional leads, bid-support resources and local representatives. Evaluation will consider relevant experience, language capability, geographic presence, availability and ability to mobilise resources in the proposed markets.

Compliance, integrity and protection of C-DOT's interests	10	Proposed controls relating to confidentiality, intellectual property, use of C-DOT's name and brand, accuracy of product claims, appointment of intermediaries, conflict-of-interest management, anti-bribery requirements, sanctions, export controls, data protection and compliance with Indian and destination-country requirements.
Presentation and product-market case response	5	Clarity, practicality, evidence, internal consistency and product relevance of the applicant's presentation or case response, where requested by C-DOT.
Total	**100**	

4.8 Technical Evaluation: Solution Partner

Criterion	Marks	Assessment Focus
Relevant product and integration experience	25	Comparable implemented assignments, exact role, scale, complexity, acceptance and customer evidence.
Proposed team and delivery ecosystem	20	Named technical/project resources, certifications, locations, availability and approved subcontractor ecosystem.
Solution and implementation capability	15	Architecture, sizing, integration, migration, project management, testing, acceptance and documentation capability.
Company financial capacity	15	Assessment of the applicant's financial stability based on audited financial statements, annual turnover, during the preceding three financial years
Operations and support capability	10	Helpdesk, field support, spares, monitoring, incident management, SLA delivery and escalation model.
Presentation / technical case response	10	Clarity, practicality, assumptions, risk treatment and consistency.
Security, quality, regulatory and risk controls	5	Proposed controls relating to confidentiality, intellectual property, anti-bribery requirements, sanctions, export controls, data protection and compliance with Indian and/or destination-country

Criterion	Marks	Assessment Focus
		requirements.
Total	**100**	

4.9 Minimum Technical Threshold

The minimum technical qualification cut off/ criteria is 50 marks. The applicant must score at least 50 marks in the technical evaluation for C-DOT to proceed with the next steps for their application.

4.10 Evaluation Transparency and Records

The evaluation committee will record responsiveness, pass/fail findings, scores, clarifications, verification outcomes and reasons for recommendation. Where an applicant applies for multiple product categories or both roles, each applicable result will be recorded separately. C-DOT may communicate only the outcome in the form of a list of empanelled Lead Generation Partners and Solution Partners and any score or qualification related information as approved by the competent authority may be published at C-DOT's discretion, while preserving confidentiality of competing applications and evaluation deliberations.

4.11 Reservations

- C-DOT may amend, extend, suspend, cancel or reissue the Call for Partner Empanelment; seek additional information; reject any or all applications; or decide not to proceed, subject to applicable approvals.
- C-DOT is not bound to shortlist the highest-scoring applicant or any minimum or maximum number of applicants where documented strategic, security, conflict, concentration or product-fit considerations apply.
- Material misstatement, concealment, forged evidence or unauthorised representation may result in rejection, removal from a later panel and other action available under law or contract.
- The final empanelment, commercial and project terms will be governed only by the definitive documents executed by the relevant parties.
- C-DOT reserves the right, to determine the number of applicants to be empanelled under each partner category and/or product category, based on the evaluation results, its assessed requirements, market coverage, product-specific needs and other relevant strategic considerations in scope of this empanelment process. Any such determination shall be made in a fair, transparent and non-discriminatory manner, and shall not confer upon any applicant a right to empanelment merely by reason of

meeting the minimum eligibility qualification criteria, as mentioned earlier in the document.

- C-DOT reserves the right, at its sole discretion, to increase the number of empanelled partners or empanel additional partners, based on its strategic requirements, without any obligation to provide existing em nelled partners with exclusivity or a minimum allocation of work.
- C-DOT reserves the right to periodically review the performance, compliance and continued eligibility on a half yearly basis, of each empanelled partner and may suspend, restrict or cancel empanelment for unsatisfactory performance, breach of contractual obligations, non-compliance with applicable laws, or violation of C-DOT's prescribed policies, standards or principles. Such action shall be without prejudice to any other rights or remedies available to C-DOT under the applicable agreements or law.
- Current and existing agreements with Transfer of Technology (ToT) and licensing partners with C-DOT shall remain unaffected by this Call for Partner Empanelment. However, any new agreement concerning the licensing of any technology or solution shall be governed by the revised terms and conditions formulated in accordance with this document and future empanelment process.
-

Application Forms

Annexure A: Covering Letter

Covering Letter

(To be submitted on the letter head of the company)

Date:

To
Partner Empanelment Secretariat, Marketing Department
Centre for Development of Telematics (C-DOT)
C-DOT Campus, Mehrauli, New Delhi – 110030

Subject: Submission of response to Call for Partner Empanelment for Lead Generation Partners and Solution Partners for C-DOT Products

Dear Sir,

Having read the Call for Partner Empanelment document bearing reference number [Text here], date [Text here] released by C-DOT, we, undersigned, hereby acknowledge the receipt of the same and offer the interest of our organisation for empanelment as a [Text here] (Lead Generation Partner / Solution Partner) for C-DOT in conformity with the said document.

We undertake to abide by all the terms and conditions mentioned in the said Call for Partner Empanelment and intend to participate in subsequent formalities.

We hereby declare that all the information and supporting documents furnished as a part of our response to the said Call for Partner Empanelment, are true to the best of my knowledge. We understand that in case any discrepancy is found in the information submitted by us, our application will be liable to be rejected.

The submission forms and all supporting documents have been uploaded on the portal.

(Signature)

Name:

Designation:

Organisation Name:

Registered Address:

(Company Stamp/Seal)

Annexure B: Common Application Form

Complete this form once, irrespective of the number of product categories selected. The Common Application Form is provided for reference; the Applicant shall make the corresponding submission through the portal notified by C-DOT.

Note: The form mentioned here is representative for reference of the applicant. Please refer the actual application available on the portal in the link mentioned in the start of the document.

Annexure B1. Applicant General Information Form

Note: Fields identified as conditional are to be completed only when triggered by the related Yes/No response on the portal.

Field	Applicant Response	Document Treatment
Legal name of Applicant	*[Enter the legal name of the firm exactly as stated in the Certificate of Incorporation or Registration]*	Direct upload: Certificate of Incorporation or Registration under Annexure B1.
Legal status	*[Select the Applicant firm's legal status]*	No separate upload. To be supported by the Certificate of Incorporation or Registration and applicable constitutional documents uploaded under Annexure B1.
Incorporation or registration number	*[Enter the incorporation or registration number]*	No separate upload. To be supported by the incorporation or registration documents uploaded under Annexure B1.
Country of incorporation or registration	*[Select the country of incorporation or registration]*	No separate upload.
Place of incorporation or registration	*[Enter the city and state, province or region]*	No separate upload.

Field	Applicant Response	Document Treatment
Date of incorporation or registration	*[Select the date of incorporation or registration]*	No separate upload. To be supported by the incorporation or registration documents uploaded under Annexure B1.
Operating history	*[System-calculated completed period of operations up to the Call for Partner Empanelment closing date]*	No separate upload. Where the incorporation or registration documents do not establish the prescribed operating history, reference the annual statutory filings, annual reports, corporate-registry extracts or equivalent evidence uploaded under Annexure B1.
Registered office address	*[Enter address line, city, state/province, postal code and country]*	No separate upload.
Corporate office same as registered office	*[Select Yes or No]*	No separate upload. If “Yes” is selected, the portal shall populate the registered-office address in the Corporate Office Address field.
Corporate office address	*[Enter the corporate office address if different from the registered office]*	No separate upload. Required only where the corporate office is different from the registered office.
Website	*[Enter the official website address or select “No official website”]*	No upload.

Field	Applicant Response	Document Treatment
Tax and statutory registrations	*[Add each applicable registration separately, including registration type, number, issuing authority, country and validity]*	Direct upload for each record: applicable tax, business, trade or statutory registration certificate. Indian Applicants shall include PAN, GST and IEC, where applicable; international Applicants shall provide equivalent registrations under Annexure B1.
Authorised signatory’s full name	*[Enter the full name of the authorised signatory]*	No separate upload.
Authorised signatory’s designation	*[Enter the designation]*	No separate upload.
Authorised signatory’s email	*[Enter the official email address]*	No separate upload.
Authorised signatory’s country code	*[Select the country calling code]*	No separate upload.
Authorised signatory’s telephone number	*[Enter the number without the country code]*	No separate upload.
Authorised signatory document reference	*[Select the uploaded authorisation document]*	Upload the signed Authority Letter prescribed at Annexure E together with the Board Resolution, Power of Attorney, Letter of Authorisation or equivalent legally valid document, as applicable.
Primary Partner contact same as authorised signatory	*[Select Yes or No]*	No upload. If “Yes” is selected, the portal shall populate the authorised signatory’s details in the Primary PARTNER Contact fields.

Field	Applicant Response	Document Treatment
Primary PARTNER contact’s full name	*[Enter the full name]*	No upload. Required only where the Primary PARTNER Contact is different from the authorised signatory.
Primary PARTNER contact’s designation	*[Enter the designation]*	No upload. Required only where the Primary PARTNER Contact is different from the authorised signatory.
Primary PARTNER contact’s email	*[Enter the official email address]*	No upload. Required only where the Primary PARTNER Contact is different from the authorised signatory.
Primary PARTNER contact’s country code	*[Select the country calling code]*	No upload. Required only where the Primary PARTNER Contact is different from the authorised signatory.
Primary PARTNER contact’s telephone number	*[Enter the number without the country code]*	No upload. Required only where the Primary PARTNER Contact is different from the authorised signatory.
Existing or previous association with C-DOT	*[Select Yes or No]*	No mandatory upload. If “Yes” is selected, complete the Nature of Association and C-DOT Association Details fields below.
Nature of association with C-DOT	*[Select all applicable association types: Technology Transfer; Licence; Customer; Vendor; Project Engagement; Research Collaboration; MoU; PoC/Trial; Previous EOI/Bid; Other]*	Optional supporting upload: agreement, work order, licence, MoU, completion record or other relevant record. Required only where an existing or previous association is declared.

Field	Applicant Response	Document Treatment
C-DOT association details	*[Provide the relevant product or project, document/reference number, period and present status]*	Optional supporting upload: agreement, work order, MoU, completion record or other relevant evidence. Required only where an existing or previous association is declared.
Applicant’s brief profile	*[Provide an overview of the Applicant, its history, scale and principal capabilities]*	Optional upload: corporate profile or annual report.
Employee strength	*[Select the current employee-strength range]*	No upload.

Annexure B2. Product-Category and Role Selection

No.	Product Category	Role Selection
1	Mobile Communications	☐ Lead Generation Partner ☐ Solution Partner
2	Private 5G	☐ Lead Generation Partner ☐ Solution Partner
3	Telecom Fraud Management	☐ Lead Generation Partner ☐ Solution Partner
4	Enterprise Cybersecurity	☐ Lead Generation Partner ☐ Solution Partner
5	Central Equipment Identity Register	☐ Lead Generation Partner ☐ Solution Partner
6	Centralised International Outroamer Register	☐ Lead Generation Partner ☐ Solution Partner
7	Internet Traffic Analyser	☐ Lead Generation Partner ☐ Solution Partner
8	Quantum Communications: QKD and Sub-systems	☐ Lead Generation Partner ☐ Solution Partner
9	Quantum Communications: PQC	☐ Lead Generation Partner ☐ Solution Partner

No.	Product Category	Role Selection
10	Disaster Management	☐ Lead Generation Partner ☐ Solution Partner
11	Mission Critical Communications	☐ Lead Generation Partner ☐ Solution Partner
12	Digital Intelligence Platform	☐ Lead Generation Partner ☐ Solution Partner

Annexure B3. Common Pre-Qualification Response

Ref.	Criterion	Comply	Evidence File and Page
PQ-1	Legal existence	☐ Yes ☐ No	
PQ-2	Operating history	☐ Yes ☐ No	
PQ-3	Financial capacity	☐ Yes ☐ No	
PQ-4	Solvency	☐ Yes ☐ No	
PQ-5	Debarment and integrity	☐ Yes ☐ No	
PQ-6	Tax and statutory compliance	☐ Yes ☐ No	
PQ-7	Ownership disclosure	☐ Yes ☐ No	
PQ-8	Conflict disclosure	☐ Yes ☐ No	
PQ-9	Litigation and regulatory disclosure	☐ Yes ☐ No	
PQ-10	Authorisation and validity	☐ Yes ☐ No	
PQ-11	Confidentiality and verification	☐ Yes ☐ No	
PQ-12	International applicability	☐ Yes ☐ No	

Annexure B4. International Experience and Presence

Country	Nature of Presence / Partner Arrangement	Since	Relevant Sectors / Customers	Evidence

Annexure C: Product-Category Response Form

Submit one separate copy of this form for every product category selected in Annexure B. Do not combine multiple product categories in one Annexure C.

Annexure C1. Product Category Form

Field	Applicant Response
Product category and number	
Products/solutions included	
Role applied for: Lead Generation Partner / Solution Partner	
Target countries	
Target customer segments	
Applicant’s understanding of the product category and principal use cases	
Relevant completed assignments	
Current market presence and customer ecosystem	
Product-specific market-entry and opportunity-development approach	
Product-specific solution and implementation approach	
Third-party components, local partners and subcontractors	
Regulatory, licensing, certification, export and security approach	
Proposed key team and locations	
First-line support, field service and escalation model	

Field	Applicant Response
First 12-month activity and opportunity plan	
Principal assumptions, dependencies and risks	
Competing products, principal relationships and conflicts	
Evidence index	

Annexure C2. Comparable Assignments

No.	Customer / Country	Period	Technology / Product	Applicant Role	Scope, Outcome and Evidence
1					
2					
3					
4					
5					

Annexure C3. Product-Specific Mandatory Gate

Requirement	Comply	Evidence File and Page
Applicant meets the product-category gate stated in Section 3.3.	☐ Yes ☐ No	
Applicant meets the role-specific gate for every role selected.	☐ Yes ☐ No	
Required team and delivery/market resources are available.	☐ Yes ☐ No	
Competing relationships and conflicts are fully disclosed.	☐ Yes ☐ No	

Annexure D: Document Checklist

No.	Document	Applicability	Applicant File and Page
1	Signed covering letter	All	
2	Common Application Form	All	
3	Certificate of incorporation/registration and constitutional documents	All	
4	Tax and statutory registrations	All	
5	Audited financial statements for latest three completed financial years	All	
6	Turnover and net-worth certificate	All	
7	Authorised-signatory document	All	
8	Beneficial ownership and affiliate declaration	All	
9	Debarment, insolvency, litigation and integrity declarations	All	
10	Conflict and competing relationship disclosure	All	
11	Separate Product-Category Form for each selected category	As applicable	
12	Project credentials and customer evidence	As applicable	
13	Market/country evidence and mobilisation plan	As applicable	
14	Certifications and accreditations, as applicable	As applicable	
15	English translations of supporting documents, as applicable	As applicable	

Annexure E: Authority Letter

Authority Certificate

(To be submitted on company's letter head)

Reference: Document No.: [Text here]

Date:

To
Partner Empanelment Secretariat, Marketing Department
Centre for Development of Telematics (C-DOT)
C-DOT Campus, Mehrauli, New Delhi – 110030

Dear Sir,

We, M/s _____ (Name of the firm) having its registered office at _____ (address of the firm) herewith submit our proposal against the aforementioned Call for Partner Empanelment document.

Mr./Ms. _____ (Name and designation of the authorised signatory), resident of _____ _____ (address of the authorised signatory), whose signature is appended below, is authorised to sign and submit the proposal documents and all other relevant documents pertaining to this empanelment on behalf of _____ _____ (name of the firm) against the said Call for Partner Empanelment.

Specimen Signature: _____

The undersigned is authorised to issue such authorisation on behalf of us.

For and on behalf of M/s _____ (name of the firm)

(Signature)

Name:

Designation:

Organisation Name:

Registered Address:

(Company Stamp/Seal)

Annexure F: Financial Strength of the Organisation

Financial Strength Declaration

(To be submitted on the letter head of the Auditor/ Chartered Accountant)

(To be signed and stamped by the respective Auditor / Chartered Accountant)

(For foreign entities, the turnover, net profit, and net worth must be given in a freely convertible currency at the exchange rate prevailing on the date of issuance of this Call for Partner Empanelment.)

Reference: Document No.: [Text here]

Financial Strength of the Organisation				
S. No.	Financial Year	Annual Turnover	Annual Net Profit	Net Worth
1.	2023-24			
2.	2024-25			
3.	2025-26			

(Signature)

Name:

Designation:

Organisation Name:

Registered Address:

(Company Stamp/Seal)

Annexure G: Integrity Certificate

Integrity Certificate

(To be submitted on company's letter head

Reference: Document No.: [Text here]

Date:

To
Partner Empanelment Secretariat, Marketing Department
Centre for Development of Telematics (C-DOT)
C-DOT Campus, Mehrauli, New Delhi – 110030

Dear Sir,

I, _____ (name of the authorised signatory), son/daughter of _____ _____, residing at _____ (address of the authorised signatory, working at M/s _____ (name of the firm) having its registered office at _____ (address of the firm), in the capacity of _____ (designation of the authorised signatory), hereby certify that no employee of C-DOT involved in this Business Partner empanelment has any shareholding or financial interest/stake at our company/organisation.

We further declare that:

- The applicant is not relying on personnel, affiliates, credentials or resources that will not be available for implementation of the proposed engagement.
- All material ownership, conflict, litigation, debarment, insolvency and regulatory matters have been disclosed.
- No unauthorised payment, inducement or representation has been made in connection with this Call for Partner Empanelment.
- The applicant accepts that this Call for Partner Empanelment does not constitute empanelment, exclusivity, a territory allocation, an assurance of business or authority to represent C-DOT.
- C-DOT may verify submitted information, contact references and undertake due diligence.
- The applicant will comply with confidentiality, intellectual-property, security, integrity and applicable legal requirements.

In case, at any stage, it is found that the information given by me is false/incorrect, C-DOT shall have the absolute right to take any action as deemed fit with a defined prior intimation to me.

In case, at any stage, it is found that the information given by me requires any update, the same shall be informed without delay.

For and on behalf of M/s _____ (name of the firm)

(Signature)

Name:

Designation:

Organisation Name:

Registered Address:

(Company Stamp/Seal)

Annexure H: Declaration of Blacklisting and Debarment

Non-Blacklisting Certificate

(To be submitted on company's letter head

Reference: Document No.: [Text here]

Date:

To
Partner Empanelment Secretariat, Marketing Department
Centre for Development of Telematics (C-DOT)
C-DOT Campus, Mehrauli, New Delhi – 110030

Dear Sir,

This is to notify you that our firm/ company/ organisation M/s _____ (name of the firm) intends to submit a proposal in response to the above referred Call for Partner Empanelment for intending to be selected for empanelment as Business Partner for C-DOT. In accordance with the above we declare that:

a. We are not involved in any major litigation that may have an impact of affecting or compromising the terms of the collaboration as required under this Call for Partner Empanelment.
b. We are not blacklisted by any Union/State Government/ agency of Union/ State Government of India or any other country in the world/ Public Sector Undertaking/ any Regulatory Authorities or a Multilateral firm in India or any other country in the world for any kind of fraudulent activities as on date of submission of this response.

For and on behalf of M/s _____ (name of the firm)

(Signature)

Name:

Designation:

Organisation Name:

Registered Address:

(Company Stamp/Seal)

Annexure I: Declaration of Solvency

Solvency Declaration

(To be submitted on company's letter head)

Reference: Document No.: [Text here]

Date:

To
Partner Empanelment Secretariat, Marketing Department
Centre for Development of Telematics (C-DOT)
C-DOT Campus, Mehrauli, New Delhi – 110030

Subject: Declaration Regarding Solvency and Non-Insolvency Status

Dear Sir,

We hereby declare and certify that:

- M/s _____ [name of the firm] is a legally constituted entity and is financially sound and capable of performing the obligations under the proposed contract.
- We are not insolvent, bankrupt, wound up, under liquidation, under receivership, or under any proceedings for insolvency, bankruptcy, liquidation, or administration, whether voluntary or compulsory.
- No application, petition, or proceeding has been filed or is pending against us under the provisions of the Insolvency and Bankruptcy Code, 2016 (IBC) or any other applicable law relating to insolvency, liquidation, or restructuring that would materially affect our ability to perform the contract.
- We have not suspended payments to creditors and are not subject to any arrangement with creditors that would impair our financial capacity to execute the assignment.
- We undertake to immediately notify the Authority if any event occurs after submission of the application that may affect the truthfulness of this declaration.
- We understand that submission of any false declaration may lead to rejection of our application, termination of empanelment, and any other action deemed appropriate by the Authority.

We hereby certify that the above statements are true and correct to the best of our knowledge and belief.

For and on behalf of M/s _____ (name of the firm)

(Signature)

Name:

Designation:

Organisation Name:

Registered Address:

(Company Stamp/Seal)

Annexure J: Products Concept Notes

[This page has been left blank on purpose. The product concept notes are appended ahead.]

4G, 5GNSA Core & Open RAN Solutions

1. Introduction

As India pursues Atmanirbhar Bharat in telecom, C-DOT has developed fully indigenous 4G and 5G core and RAN solutions. These technologies offer strategic independence, cost-efficiency, and network security, while aligning with international standards for wide applicability across diverse network environments.

2. Product Overview

C-DOT's 4G Core is a converged, 3GPP-compliant, cloud-based, and virtualized solution catering to mobile, fixed line/FTTH, and Wi-Fi services. It is already deployed in a major Indian operator's commercial network and is under PoC for critical infrastructure like national railways. The 4G RAN solution includes mass-manufacturable, macro-class radios supporting multiple frequency bands and is TEC-certified.

C-DOT's 5G NSA Core builds on the 4G Core to offer high-speed, premium 5G services with low latency and robust security. A 5G SA Core is under development. The 5G Open RAN ("Bharat RAN") is a modular, disaggregated architecture developed in collaboration with industry partners, enabling cost-effective, secure, and flexible 5G deployments.

USPs include full indigenous development, cloud-native architecture, hardware agnosticism, and scalability. The key benefits are low CAPEX/OPEX, elimination of expensive vendor lock-in, and ease of integration for private and public network use cases.

3. Unique Strengths and Benefits

- Strategic autonomy: Reduces dependence on traditional telecom vendors
- Cost efficiency: Optimized CAPEX and OPEX for operators
- Scalable: Supports deployment across diverse network sizes and use cases
- Secure: Built with indigenous design for enhanced network trust and resilience
- Flexible integration: Compatible with public, private, and captive network environments

4. Objectives

The solutions aim to ensure national telecom self-reliance, reduce foreign dependency, and provide scalable, secure, and affordable telecom infrastructure for use in commercial, captive, and critical mission networks across India and other emerging markets. • Achieve national self-reliance in telecom infrastructure

- Reduce dependency on traditional technology ecosystems
- Enable scalable, secure, and affordable connectivity solutions
- Support deployment across commercial, enterprise, and critical mission networks

5. Implementation Approach

The 4G Core has been rolled out pan-India in a major mobile operator's commercial network and also tested on national railways infrastructure. It has also received TEC certification. C-DOT has also signed a Transfer of Technology (ToT) Agreement with select domestic manufacturers. The 5G NSA Core has been deployed in select location(s) of a major mobile operator in India. SA Core to be ready soon. 5G Open RAN has been developed in collaboration with industry and is under trial in a major

mobile operator’s environment. Meanwhile indoor/outdoor testbeds and OTIC labs has been set up at CDOT Delhi and Bengaluru.

6. Use Cases

- **Telecom operators**: Secure and large-scale public mobile networks
- **Critical infrastructure**: Railways, utilities, and defence networks requiring high reliability
- **Enterprises**: Private 5G networks for industrial automation and campuses
- **Rural broadband**: Cost-effective connectivity for remote and underserved areas
- **International markets**: Trusted and indigenous alternative for countries seeking secure 4G deployments

7. Way Forward

C-DOT plans commercial rollout of the 5G NSA Core and 5G Bharat RAN in collaboration with public and private partners. Further enhancements include finalizing the 5G SA Core, scaling up manufacturing for 4G/5G radios, and offering these technologies for export and strategic international collaborations in regions like Africa, Southeast Asia, and Latin America.

Private 5G Solution

Introduction

Communication plays an important role in refineries, ports, mines and other enterprises, where it supports the monitoring of worker safety and increases operational efficiency.

Refineries, ports and mines are highly regulated environments where safety is a top priority. CDOT's Private 5G Solution delivers a reliable communication channel for monitoring user safety and increasing operational efficiency in these areas, making it fully suitable for refineries, ports, mines and other enterprise markets.

2. Product Overview

C-DOT's Private 5G Solution is an indigenously designed private 5G network solution, compliant with 3GPP Release 15 and O-RAN standards. It is suitable for enterprises and private 5G applications, and provides cost-effective, affordable and secured 5G services to end users. The solution integrates MCX features, 5G IoT devices and sensors to enable monitoring of user safety and increased operational efficiency.

Key System Features

- 3GPP Release 15 and O-RAN compliant
- O-RAN 7.2a split
- Band 78 (TDD)
- MIMO 4T4R, 30 kHz SCS support
- Modulation support up to 256 QAM
- Bandwidth support up to 100 MHz

3. Unique Strengths and Benefits

- **Cost effective:** Affordable and secured 5G services for end users
- **Integrated solution:** Combines MCX features, 5G IoT devices and sensors
- **Central monitoring:** Dashboard for sensor data and IoT use cases, with real-time monitoring, alerts
- **Standards-based:** O-RAN compliant and indigenously designed
- **Scalable:** Can be scaled as per customer requirements
- **Reliable communication:** Channel for monitoring user safety and increasing operational efficiency

4. Objectives

- Provide a reliable communication channel for monitoring user safety
- Increase operational efficiency in refineries, ports, mines and other enterprise markets
- Deliver cost-effective, affordable and secured 5G services to end users
- Enable central, real-time monitoring and alerts for sensor data and IoT use cases

5. Implementation Approach

The solution is delivered as an O-RAN compliant private 5G network that integrates MCX features, 5G IoT devices and sensors. A central monitoring dashboard presents sensor data and IoT use cases for real-time monitoring and alerts, and the solution can be scaled as per customer requirements.

6. Use Cases

C-DOT's Private 5G Solution supports the following use cases:

- **Captive Non-Public Networks (CNPN):** 5G captive networks for refineries, ports and mines
- **Smart helmets:** 5G-enabled smart helmets
- **Video analytics:** 5G-enabled cameras for video analytics

- **Government strategic bodies:** Captive private 5G network solution
- **Urban areas – Public safety:** Surveillance (smart cities), infrastructure management and maintenance
- **Urban areas – Media and entertainment:** UHD video streaming
- **Rural areas – Healthcare:** Telemedicine and wearable devices
- **Rural areas – Agriculture:** Precision farming, crop monitoring using drones, smart livestock management
- **Rural areas – Education:** Smart classrooms and skill training

FraudPro: AI/ML-Powered Telecom Fraud Detection

Introduction

With the rapid growth of digital connectivity, telecom networks have become a key vector for financial fraud, identity theft, and cybercrime. Addressing this challenge, C-DOT has developed FraudPro, an AI/ML-powered fraud detection platform designed to identify and eliminate fraudulent mobile connections at scale.

By leveraging advanced machine learning and computer vision techniques, FraudPro detects SIM registrations using morphed photographs and forged identity documents, two of the most common fraud methods. Successfully deployed in India, the solution has enabled the disconnection of over **20 million** fraudulent connections, significantly strengthening national security and consumer protection.

2. Product Overview

FraudPro is a comprehensive, end-to-end fraud detection framework that integrates seamlessly with telecom operators' infrastructure to enable real-time identification and mitigation of fraudulent connections.

Key features include:

- AI/ML-driven detection of fraudulent SIM registrations using image and document analysis
- Computer vision models to identify morphed photographs and digital manipulation
- Automated anomaly detection and real-time flagging of suspicious subscriber data
- Seamless integration with Telecom Service Providers (TSPs) for rapid disconnection
- Scalable architecture capable of processing millions of subscriber records
- Centralized platform enabling coordination with law enforcement agencies
- Continuous learning models adapting to evolving fraud patterns

3. Unique Strengths and Benefits

- **AI-driven intelligence:** Advanced ML and computer vision ensure high detection accuracy with minimal false positives
- **Proven at scale:** Successfully deployed in India with over 20 million fraudulent connections eliminated
- **Proactive fraud prevention:** Detects and neutralizes fraudulent numbers before misuse
- **Seamless ecosystem integration:** Works across multiple telecom operators for coordinated action
- **Adaptive learning:** Continuously evolving models to counter emerging fraud techniques
- **National security impact:** Reduces anonymous and untraceable communication channels
- **Global replicability:** Scalable and exportable model for international adoption

4. Objectives

- Detect and eliminate fraudulent mobile connections at scale
- Prevent misuse of telecom networks for financial fraud and cybercrime
- Enable real-time, coordinated disconnection across telecom operators
- Strengthen national security and consumer protection frameworks
- Support law enforcement with actionable intelligence
- Build a continuously evolving AI-driven fraud detection ecosystem
- Position FraudPro as a globally adoptable telecom fraud solution

5. Use Cases

- **Fraudulent SIM detection:** Identification and disconnection of unauthorized mobile connections
- **Financial fraud prevention:** Reducing OTP fraud, digital payment scams, and banking frauds
- **Identity theft mitigation:** Preventing misuse of forged identity documents

- **Law enforcement support:** Providing intelligence for investigation and prosecution
- **National security:** Eliminating anonymous connections used for criminal activities
- **Spam & phishing reduction:** Curtailing large-scale fraudulent communication campaigns

6. Way Forward

C-DOT plans to further enhance and expand FraudPro as a next-generation telecom fraud prevention platform:

- Transition towards **real-time detection at SIM registration stage**
- Enhancement of AI/ML models for detecting advanced fraud techniques
- Integration with financial institutions, digital platforms, and regulators
- Development of predictive analytics for early fraud detection
- Expansion into international markets as a scalable fraud prevention solution
- Strengthening cross-border collaboration to combat global telecom fraud
- Contribution to regulatory frameworks and global best practices in AI-driven fraud detection

TRINETRA: AI-powered Unified Cyber Security Solution for Enterprises

1. Introduction

Cyber threats have rapidly evolved from basic malware to sophisticated, multi-vector attacks targeting endpoints, networks, users, and cloud workloads. Organizations today face challenges of growing complexity, stringent compliance requirements, and the need for resilient operations. C-DOT has developed TRINETRA, **an indigenous, AI-driven Unified Cyber Security Platform** that consolidates multiple security technologies into a single, integrated ecosystem. Purpose-built for enterprises, government bodies, and critical sectors, TRINETRA delivers real-time threat detection, prevention, response, and compliance management while aligning with national security and data sovereignty priorities.

2. Product Overview

TRINETRA addresses vulnerabilities created **by fragmented tools, limited automation, and dependency on foreign OEMs**. It provides an end-to-end, modular, and fully integrated platform for enterprise-wide cybersecurity. **Key Highlights**

- **Comprehensive coverage:** Endpoints, networks, users, applications, and data
- **AI-powered detection:** Identifies known and unknown threats with high accuracy
- **Integrated platform:** Eliminates silos and reduces operational complexity
- **Regulatory compliance:** Supports CERT-In, ISO 27001, and other global frameworks
- **Flexible deployment:** On-premise, cloud, or hybrid options

3. Unique Strengths and Benefits

- **Unified visibility & control:** Single console view across endpoints, networks, and users
- **Rapid incident response:** SOAR-enabled playbooks reduce detection and response times
- **Data sovereignty:** Fully indigenous solution aligned with India's security priorities
- **Compliance assurance:** In-built audit, benchmark, and compliance modules
- **Lower total cost of ownership:** Reduces dependency on multiple vendor tools
- **Scalability:** Suitable for SMEs, large enterprises, and national-level deployments

4. Objectives

TRINETRA reflects C-DOT's vision of a **secure, resilient, and self-reliant digital ecosystem**.
Objectives:

- Provide holistic, AI-powered cybersecurity for enterprises and government agencies
- Enable rapid detection and response to sophisticated multi-vector attacks
- Support regulatory compliance and strengthen cyber resilience
- Reduce foreign dependency by offering an indigenous alternative to OEM tools
- Extend India's cyber defence capabilities to international partners

5. Implementation Approach

The solution combines modular components into a unified, AI-driven platform.

Key Components

- Unified Endpoint Management (UEM)
- Endpoint Detection & Response (EDR)
- Data Loss Prevention (DLP)

- Network Detection & Response (NDR)
- Security Information & Event Management (SIEM)
- Security Orchestration, Automation & Response (SOAR)
- User & Entity Behavior Analytics (UEBA)
- Security Audit, Benchmark & Compliance (SABC)

6. Use Cases

- **Government:** Secure critical networks and ensure compliance with CERTIn directives
- **Enterprises & PSUs:** Prevent data leakage, insider threats, and advanced persistent threats
- **Critical infrastructure:** Protect national defence, transport, and energy sectors
- **Financial institutions:** Safeguard sensitive financial data and customer information
- **Academia & R&D:** Ensure safe digital operations and protect intellectual property

7. Way Forward

Building on current success, the roadmap for TRINETRA includes:

- **Scale:** Expand adoption across central/state government agencies, PSUs, and enterprises
- **Innovate:** Integrate advanced AI/ML models for predictive threat intelligence
- **Collaborate:** Engage with regulators and global partners to harmonize cybersecurity standards
- **Export:** Position TRINETRA as a secure, indigenous cybersecurity solution for friendly nations

TRINETRA strengthens India’s cyber defence posture and positions C-DOT as a leader in indigenous cybersecurity innovation, offering trusted solutions for both domestic and global markets.

Lost/Stolen Handset Tracking and Blocking (CEIR)

1. Introduction

With rapid growth in mobile usage, theft, IMEI cloning, and counterfeit handset circulation have emerged as major threats to citizens and telecom networks.

C-DOT has developed the **Centralized Equipment Identity Register (CEIR)**, an indigenous platform that connects to the IMEI databases of all mobile operators in India. It enables real-time blocking of stolen/lost devices, ensuring that unauthorized handsets cannot operate on any network, even if the SIM is changed.

Through a citizen-friendly online portal, mobile app, and law enforcement interface, CEIR empowers users to report stolen devices. Blocked devices are barred across all Indian networks, while traceability reports support law enforcement in tracking attempted usage of stolen phones.

2. Product Overview

CEIR is a centralized, secure system designed to combat handset theft and ensure device authenticity nationwide.

Key Highlights

- Real-time blocking of stolen/lost handsets across all Indian networks
- Seamless citizen reporting via portal, app, or SMS
- Traceability of blocked devices for law enforcement
- Detection and blocking of counterfeit and cloned devices
- Device authentication system ensuring only genuine handsets operate
- GSMA-linked TAC database for continuous device validation

3. Unique Strengths and Benefits

- **Citizen empowerment:** Easy reporting and quick blocking of lost/stolen devices
- **Law enforcement support:** Traceability reports aid investigations and recovery
- **Consumer protection:** Verification of handset authenticity before purchase via KYM tool
- **National security:** Restricts cloned and counterfeit devices through ICDR compliance
- **Trusted ecosystem:** Ensures only legitimate handsets operate on national networks
- **Scalable design:** Proven success in India, adaptable for international adoption

4. Objectives

- Prevent unauthorized devices from accessing telecom networks
- Assist citizens and authorities in recovering stolen devices
- Safeguard consumers from counterfeit or cloned handsets
- Strengthen national security by curbing illegal device circulation
- Establish a verifiable ecosystem for handset authentication

5. Use Cases

- **Citizens:** Report and block stolen handsets, verify authenticity before purchase
- **Telecom Operators:** Maintain clean networks by blocking unauthorized devices
- **Law Enforcement Agencies:** Trace stolen devices and support investigations
- **Governments:** Prevent counterfeit device imports, enforce regulatory compliance
- **International Partners:** Adapt CEIR to emerging markets facing handset theft and counterfeit challenges

6. Way Forward

Building on its success in India, CEIR is positioned for broader deployment internationally. The roadmap includes:

- Collaboration with countries in Africa and other regions with rising mobile penetration
- Linking with customs databases and handset dealers to curb illegal imports
- AI-driven analytics for fraud detection and device misuse trends
- Promote CEIR as a scalable, indigenous solution for mobile security worldwide

Cross-Border Spoofed CLI Call Blocking Solution

1. Introduction

Spoofed international calls, where fraudsters manipulate the Calling Line Identification (CLI) to appear as local numbers, have become a major telecom security concern worldwide. Such calls are frequently exploited for financial fraud, scams, and identity theft, undermining citizen safety and eroding trust in communication systems.

C-DOT has developed an **indigenous Cross-Border Spoofed CLI Call Blocking Solution**, designed to detect and block spoofed calls in real time. By ensuring only authentic communications reach subscribers, this solution strengthens national security and safeguards consumer trust, while offering strong potential for international deployment.

2. Product Overview

The solution uses advanced algorithms to analyse and validate CLI information on incoming international calls. Fraudulent spoofed calls are identified and blocked automatically before they reach subscribers, while legitimate international traffic is preserved without disruption.

Key Highlights

- Real-time detection and blocking of spoofed international calls
- Zero disruption to legitimate cross-border communications
- Seamless integration with operator networks
- Configurable for diverse telecom infrastructures and regulatory frameworks

3. Unique Strengths and Benefits

- **Real-time protection:** Pre-emptive blocking of spoofed calls before subscriber delivery
- **Trusted communications:** Preserves confidence in telecom services by eliminating fraud
- **Scalable:** Suitable for networks of varying size and complexity
- **Adaptive:** Algorithms continuously updated to counter evolving spoofing techniques
- **Proven in India:** Successfully operational with measurable results

4. Objectives

- Prevent fraudulent exploitation of spoofed local numbers
- Enhance citizen safety and public confidence in telecom services
- Provide telecom operators with a standards-compliant tool to counter spoofing
- Extend indigenous telecom security capabilities to friendly nations through collaboration

5. Use Cases

- **Telecom Operators:** Secure networks against fraudulent cross-border traffic
- **Regulators:** Strengthen national-level telecom security frameworks
- **Financial Sector:** Reduce scam and phishing attempts targeting consumers
- **Public Safety Agencies:** Safeguard critical communications channels
- **International Cooperation:** Support partner countries in combating global telecom fraud

6. Way Forward

Building on its successful deployment in India, the roadmap for the Cross-Border Spoofed CLI Call Blocking Solution includes:

- Broaden deployments across regions affected by telecom fraud
- Incorporate AI/ML-driven predictive detection techniques
- Partner with regulators, governments, and global telecom operators
- Position India as a global hub for indigenous telecom security solutions

C-DOT's solution represents a decisive step in combating telecom fraud, ensuring secure and trusted communication networks for India and the world.2

C-DOT Network Traffic Probe (IPFIX)

1. Introduction

Telecom and IP networks keep growing in size, speed and complexity. Knowing what is actually happening on them, in real time, is now essential for performance, security, regulatory compliance and day-to-day network management. Sampling-based monitoring often falls short here. It can miss the traffic details needed to spot anomalies, understand application behaviour or support forensic work.

C-DOT has developed an indigenous Network Traffic Probe to close that gap. It sits passively on a network link without requiring changes to network routing, processes traffic at line rate without sampling, and turns raw packets into enriched flow records based on IPFIX standards. The records can be exported to downstream network monitoring, security analytics, SIEM, NDR, performance monitoring, observability, compliance monitoring and data analytics platforms for correlation and long-term analysis.

The solution is designed as a scalable and standards-compliant platform and can be deployed across large-scale ISPs, government, security zones and national network infrastructure.

2. Product Overview

The C-DOT Network Traffic Probe (IPFIX) is a high-performance, passive network monitoring solution engineered for large-scale and high-throughput network environments. It captures, inspects and generates flow records from traffic at full line rate, with no changes to network routing and no effect on Quality of Service (QoS).

The probe converts raw network traffic into enriched flow-based metadata and exports it in IPFIX format. It has capabilities to provide visibility from Layer 3 through Layer 7, including application and protocol-level characteristics with Deep packet inspection (DPI) without violating users' privacy.

DPI also identifies applications that do not use their expected ports, which port-based classification misses. For encrypted traffic, the probe derives what it can from observable. This supports security, performance, troubleshooting and traffic intelligence use cases beyond conventional flow monitoring.

The probe with its flexible architecture has **rapid L7 customization with tailored output** mapped to SOC analyst requirements including AI/ML models. Another feature of probe is **universal multi-vendor interoperability** due to compliance to IPFIX standards with support to native C-DOT IPFIX collector. Other features include load balancing across multiple IPFIX collectors with or without sampling, EMS/NMS etc.

The platform therefore provides a consolidated telemetry layer between the network infrastructure and analytical systems, reducing the need for multiple independent monitoring probes while providing both conventional flow visibility and rich application-aware metadata.

Unique Strengths and Benefits

- Real-time, unsampled traffic visibility for high-speed networks
- Passive, non-intrusive deployment without routing changes or impact on QoS
- Line-rate processing of up to 200G/400G traffic in a single appliance
- Deep Packet Inspection (DPI) Layer 3 to Layer 7 traffic analysis and port independent protocol identification
- Rapid customization of DPI signatures and protocol detection based on deployment requirements
- Standards-based interoperability compliant with IETF IPFIX RFC 7011 and RFC 7012
- Enriched IPFIX flow generation with standard and customized flow attributes
- Application and protocol identification for enhanced network intelligence
- Role-based access control, notifications, and audit trails for operational governance
- Integration with SIEM, data lakes, analytics, and security orchestration platforms

3. Objectives

The probe is designed to fulfil objectives:

- Provide comprehensive, real-time visibility into high-speed network traffic
- Enable network operators to identify anomalies, threats, and unusual traffic behaviour
- Support data-driven network performance monitoring and operational decision-making
- Generate enriched flow-level intelligence for security monitoring and analytics
- Strengthen capabilities for lawful interception, digital forensics, and regulatory monitoring
- Enable integration with existing multi-vendor network monitoring and security ecosystems
- Establish a scalable and future-ready network traffic visibility infrastructure
- Support indigenous technology adoption for critical telecom and digital infrastructure

The solution achieves its objectives in the following ways:

- Performance Monitoring and Troubleshooting across High-Speed Networks.
- Cybersecurity and Network Detection & Respons,
- Internet Gateway and ISP/Service Provider Monitoring.
- Application and Service Visibility.
- DPI-Based Traffic Classification and compliance monitoring.
- Capacity Planning and Network Engineering.
- Fraud, Abuse and Anomaly Analytics.
- SOC and Security Operations.
- Data-Center and Cloud Visibility.

4. Implementation Approach

The C-DOT Network Traffic Probe is designed for passive deployment across strategic network links, including ISP backbones, gateways, transit and peering links, and data centres.

The IPFIX output can be integrated with existing SIEM, NDR, SOC, network-performance-monitoring, data-lake, big-data, and security-analytics systems. The solution can therefore operate either as a standalone flow-generation platform or as a telemetry source within a larger monitoring and security ecosystem. Further, it's modular architecture allows configuration of flow attributes, DPI requirements, export policies, and collector destinations according to the operational and regulatory requirements of the deploying organization.

C-DOT can provide deployment support, configuration, customization, DPI signature updates, integration assistance, and ongoing technical support.

Key Features of Implementation

- Passive traffic interception and monitoring without routing changes
- Full line-rate, unsampled traffic processing and flow generation
- Layer 3–Layer 7 traffic visibility through DPI with application and protocol identification
- Rapid customization of protocol detection, metadata fields, and outputs based on deployment requirements
- Configurable 1: N sampling of exported IPFIX records, and load balancing across multiple collectors
- Replication of IPFIX records to the collectors of designated users
- Real-time traffic and system statistics
- Role-based GUI access with operational notifications and audit trails
- Integration with SIEM platforms, data lakes, analytics platforms, and security orchestration systems

5. Use Cases

C-DOT's Network Traffic Probe can be deployed across national, telecom, government, security zones and large enterprise network environments.

- ISP backbone monitoring Real-time visibility into traffic patterns, application behaviour, flows, and network performance across high-capacity backbone links.
- International Internet Gateway monitoring: Comprehensive traffic visibility at strategic international gateways for network intelligence, security monitoring, and regulatory requirements.
- Transit and peering links: Monitoring traffic behaviour and flow characteristics across interconnection and peering environments.

- Security Operations Centres (SOCs): Enriched flow data and Layer 7 metadata for anomaly detection, threat analysis, and integration with security analytics platforms.
- Network performance monitoring: Real-time analysis of throughput, active sessions, flow rates, packet statistics, and traffic behaviour for faster operational decision-making.
- Lawful interception and digital forensics: Generation of detailed traffic metadata to support authorized monitoring, investigation, and forensic analysis in accordance with applicable laws and regulations.
- Data retention, regulatory compliance and monitoring: Structured traffic information to support applicable audit, monitoring, and compliance requirements.
- Data centre monitoring: High-throughput traffic visibility across centralized ISP and enterprise data centre environments.
- Encrypted traffic analysis: Use of TLS metadata to support identification and analysis of encrypted traffic characteristics.
- Large enterprise network visibility: High-performance monitoring for large-scale enterprise environments requiring detailed application and traffic intelligence.

6. Way Forward

C-DOT aims to further extend the Network Traffic Probe as an indigenous network visibility and traffic intelligence platform for deployment across telecom, government, national infrastructure, and enterprise networks.

Quantum Key Distribution (QKD)

1. Introduction

With quantum computing emerging as a critical threat to conventional encryption, C-DOT has indigenously developed a **Quantum Key Distribution (QKD)** system. QKD enables secure communication by leveraging the laws of quantum mechanics, ensuring resilience against present and future cyber threats.

2. Product Overview

The QKD system establishes secure communication by generating shared, secret random keys exclusively between two endpoints (Alice - transmitter, Bob - receiver). These keys are used for encryption/decryption of data, guaranteeing unconditional confidentiality. Any eavesdropping attempt introduces anomalies, which can be instantly detected.

- Uses standard single-mode telecom fibre for quantum and classical channels
- Seamlessly integrates into existing communication networks
- Designed for high-assurance sectors where confidentiality is paramount

3. Unique Strengths and Benefits

- Unconditional security based on principles of quantum physics
- Eavesdropping detection during key exchange
- Interoperable with existing telecom infrastructures
- Indigenous design ensuring national security and reduced dependency

4. Objectives

- Secure communication infrastructure for strategic sectors
- Enable trusted national and international adoption of quantum-safe networks.
- Strengthen India’s self-reliant posture in advanced security domains

5. Use Cases

- Defence and strategic communications
- Banking, Financial Services & Insurance (BFSI)
- Healthcare and critical infrastructure
- Government and data centre networks

6. Way Forward

- Pilot deployments in strategic and commercial sectors
- Extend deployment to friendly nations facing advanced cyber threats
- Enhance interoperability and throughput for future-proof adoption
- Collaborate internationally to shape quantum security standards

Post-Quantum Cryptography (PQC) Solutions

1. Introduction

Quantum computing is emerging as a critical threat to conventional encryption. C-DOT has developed quantum-resilient encryption solutions based on post-quantum cryptography (PQC) to protect backbone networks, end-user premises and existing infrastructures against emerging quantum threats.

2. Product Overview

C-DOT's PQC solutions secure communication at multiple points in the network, from highthroughput backbone transport to end-user communication and links in existing infrastructure. They combine quantum-resilient cryptography with classical and post-quantum algorithm support, Layer 2 and Layer 3 encryption, and hybrid key exchange methods that ensure a smooth quantumsafe migration

Key features

- Encryption with ultra-low latency
- Mul -protocol 10G client interfaces
- Encryption at both client and line levels
- Encrypted alien wavelength support for brownfield deployments
- Dual algorithm support (classical + PQC) with hybrid key exchange
- Layer 2 and Layer 3 encryption
- Secure boot and authentication mechanisms
- Audio-video calling with integrated security features, compatible with IoT-M2M systems
- Lightweight, modular and pluggable design
- Forward compatibility with PQC standards
- Flexible configuration for enterprise or defence settings

3. Unique Strengths and Benefits

- Quantum-resilient cryptography for long-term protection
- Hybrid key exchange and dual algorithm support (classical + PQC) for quantum-safe migration
- 200 Gbps performance with ultra-low latency, scalable for large-scale infrastructure deployments
- Brownfield ready, supporting alien wavelengths
- Pluggable modular design for easy integration
- End-to-end secure communication with quantum resilience, backed by secure boot and authentication
- Customizable for specific mission-critical use cases
- Future-proof design across multiple sectors, compatible with smart office and IoT environments

4. Objectives

- Protect national backbone networks from advanced cyber/quantum threats
- Support transition to post-quantum cryptography across infrastructures without major infrastructure overhaul
- Enable secure communication for enterprises and governments, including at end-user premises
- Safeguard confidential communications for defence, government and enterprises
- Provide future-ready encryption for critical networks in telecom, BFSI, healthcare, power and government sectors
- Extend secure IP-based communication to smart office and IoT ecosystems

5. **Use Cases**

- National and international backbone telecom networks, and telecom networks requiring scalable secure modules
- Defence communication backbones, and defence and government offices
- Data centres and cloud operators
- Banking and financial institutions (BFSI), including safeguarding sensitive transactions
- Healthcare and power sector communication networks
- Government communication infrastructures
- Corporate enterprises with high confidentiality needs
- Smart office environments and IoT-M2M integrated ecosystems

6. **Way Forward**

- Promote large-scale adoption as a low-cost quantum-safe enabler
- Drive adoption in international markets and with international partners that have growing backbone security needs or require future-proof solutions
- Scale adoption across defence, government and enterprise environments
- Enhance throughput and multi -protocol support in future iterations
- Continuous upgrades to align with evolving PQC standards

PQC Products :

I. Qsafe-200

1. Introduction

Qsafe-200 is C-DOT's high-throughput 200 Gbps quantum-secure encryptor, designed to protect backbone networks against emerging quantum threats.

2. Product Overview

Qsafe-200 integrates post-quantum cryptography (PQC) and Dense Wavelength Division Multiplexing (DWDM) technology. It delivers ultra-low latency, scalable security across critical backbone infrastructure.

- Supports multi -protocol 10G client interfaces
- Encryption at both client and line levels
- Encrypted alien wavelength support for brownfield deployments

3. Unique Strengths and Benefits

- 200 Gbps performance with ultra-low latency
- Scalable for large-scale infrastructure deployments
- Brownfield ready, supporting alien wavelengths
- Quantum-resilient cryptography for long-term protection

4. Objectives

- Protect national backbone networks from advanced cyber/quantum threats

- Enable secure communication for enterprises and governments
- Support transi on to post-quantum cryptography across infrastructures

5. Use Cases

- National and international backbone telecom networks
- Defence communication backbones
- Data centres and cloud operators
- Banking and financial institutions

6. Way Forward

- Drive adoption in international markets with growing backbone security needs
- Enhance throughput and mul -protocol support in future iterations

Quantum Secure Smart Video IP Phone (QSVIP)

1. Introduction

The Quantum Secure Smart Video IP Phone (QSVIP) is a customer-premise solution that ensures secure, quantum-resilient audio-video communication for strategic and enterprise environments.

2. Product Overview

QSVIP integrates secure boot, authentication , and quantum-resilient communication protocols. It is customizable per user requirement and is designed for environments demanding uncompromised confidentiality.

- Supports audio-video calling with integrated security features
- Compatible with IoT-M2M systems
- Flexible configuration for enterprise or defence settings

3. Unique Strengths and Benefits

- End-to-end secure communication with quantum resilience
- Customizable for specific mission-critical use cases
- Secure boot & authentication mechanisms
- Future-ready design compatible with smart office and IoT environments
- Plug-and-play deployment for quick adoption
- Configurable as per user requirements
- Compatible with existing enterprise/IP communication networks

4. Objectives

- Provide secure communication at end-user premises
- Safeguard confidential communications for defence, government, and enterprises
- Extend secure IP-based communication to smart office and IoT ecosystems

5. Use Cases

- Defence and government offices
- Corporate enterprises with high confidentiality needs
- Smart office environments
- IoT-M2M integrated ecosystems

6. **Way Forward**

    - Introduce advanced features such as quantum-safe conferencing
    - Expand availability in international secure communication markets

Compact Encryption Module (CEM)

1. Introduction

The Compact Encryption Module (CEM) is a lightweight, pluggable, and quantum-resilient encryption unit designed for seamless integration into existing infrastructures.

2. Product Overview

CEM supports both classical and post-quantum cryptographic algorithms, with Layer 2 and Layer 3 encryption. It provides hybrid key exchange methods to ensure smooth quantum-safe migration.

- Lightweight, modular, and easy to integrate
- Suitable for telecom, BFSI, government, and healthcare networks
- Ensures forward compatibility with PQC standards

3. Unique Strengths and Benefits

- Pluggable modular design for easy integration
- Hybrid key exchange for quantum-safe migration
- Dual algorithm support (classical + PQC)
- Future-proof encryption across multiple sectors

4. Objectives

- Provide future-ready encryption for critical networks
- Enable smooth transi on to PQC without major infrastructure overhaul
- Secure communication in telecom, BFSI, healthcare, power, and government sectors

5. Use Cases

- Telecom networks requiring scalable secure modules
- BFSI for safeguarding sensitive transactions
- Healthcare and power sector communication networks
- Government communication infrastructures

6. Way Forward

- Adoption as a low-cost quantum-safe enabler
- Expand deployment across international partners requiring future-proof solutions
- Continuous upgrades to align with evolving PQC standards

Disaster Management and Early Warning Solutions

1. Introduction

Natural disasters, extreme weather events, and unforeseen emergencies pose growing risks to human lives and critical infrastructure worldwide. Timely dissemination of accurate alerts and reliable communication with citizens are vital for preparedness and response.

C-DOT, as India's premier telecom R&D organization, has developed robust, scalable, and geointelligent solutions for early warning and disaster management. These platforms have demonstrated proven effectiveness in India and are now well positioned to support international adoption, contributing to global disaster resilience efforts.

2. Product Overview

C-DOT's flagship solution in this domain is the **Integrated Alert Platform (IAP)** — a geointelligent, multi-hazard alerting system based on the ITU-defined **Common Alerting Protocol (CAP)**.

The platform empowers disaster management authorities to issue real-time alerts in multiple languages through diverse channels including SMS, Mobile Applications, Satellite Messaging, Public Sirens, Digital Signage, and Radio and TV broadcasting.

Key complementing technology is the **Cell Broadcast Solution (CBS)**, built on **3GPP standards**, which delivers targeted, location-based alerts to millions of mobile users almost instantaneously, without congesting telecom networks. This ensures life-saving communication in time-sensitive situations such as earthquakes, cyclones, tsunamis, flash floods, and lightning strikes. **Unique Strengths and Benefits**

- Geo-intelligent targeting for precise reach
- Multilingual accessibility for inclusivity
- Multi-channel alerting for reliability and redundancy
- Proven scalability in large-scale national deployments
- Global standards compliance (ITU-CAP, 3GPP)
- Operational success with **3,500+ disaster events supported** and **200+ billion** disaster alert SMS across India

3. Objectives

- Provide timely, location-specific, and reliable early warnings to citizens
- Enable disaster management authorities to act swiftly and communicate effectively
- Strengthen community preparedness and resilience
- Establish a future-ready public warning infrastructure
- Expand international cooperation in disaster resilience and emergency communication

4. Use Cases C-DOT's solutions have been effectively deployed in India and can be adapted globally. Some illustrative use cases include:

- **Cyclone-prone coastal nations**: Rapid evacuation alerts and multilingual instructions
- **Earthquake-vulnerable regions**: Instant mass notifications with localized safety advisories
- **Flood management**: Integration with hydrological monitoring for predictive alerts
- **Cross-border disaster cooperation**: Harmonized CAP-based alerts for regional resilience
- **Public safety alerts**: City-wide notifications for health emergencies, infrastructure failures, other public safety events

5. Way Forward

- **Customizing deployments** for diverse geographies and regulatory frameworks
- **Integrating AI-driven predictive analytics** and **Decision Support Systems** for enhanced forecasting
- **Exploring interoperability** with global disaster management frameworks

Through these initiatives, C-DOT aims to contribute to building resilient nations and strengthening international cooperation for inclusive disaster preparedness and response.

Mission Critical Communication (MCX) Solutions

1. Introduction

Reliable and secure communication systems are fundamental to maintaining public safety, enabling effective disaster response, and ensuring coordinated operations among emergency services. First responders including police, fire services, medical teams, disaster management agencies, and defence personnel depend on uninterrupted, real-time communication during critical situations.

Traditional public safety communication systems largely based on narrowband technologies, are limited in their ability to support modern operational needs such as real-time video, high-speed data exchange, and integrated situational awareness.

To address these evolving requirements, India is advancing next-generation broadband-based communication technologies. C-DOT, the premier telecom R&D centre based out of New Delhi, India, is developing a standards-compliant Mission Critical Communication (MCX) platform based on global 3GPP specifications. These solutions are designed to modernize public safety communication infrastructure and are well positioned to support international collaboration.

2. Product Overview

C-DOT's Mission Critical Communication (MCX) platform is a next-generation, broadband-based solution designed to provide secure, reliable, and real-time communication services for public safety agencies and emergency responders. Built in accordance with global 3GPP Mission Critical Services standards, the MCX platform operates over LTE, 5G, and future communication networks. It integrates mission-critical voice, video, and data services within a unified architecture, enabling seamless coordination across multiple agencies.

Key components of the MCX platform include:

Mission Critical Push-To-Talk (MCPTT): Enables instantaneous voice communication with ultralow call setup times for individual and group communication

Mission Critical Video (MCVideo): Supports real-time video streaming, including integration with body-worn cameras and surveillance systems

Mission Critical Data (MCData): Facilitates secure exchange of text messages, files, alerts, and operational data

The platform architecture includes MCX service servers, dispatcher systems, common services core, and user applications, enabling centralized command-and-control along with field-level communication.

3. Unique Strengths and Benefits

- Instantaneous push-to-talk communication with ultra-low latency
- Integrated voice, video, and data services on a single platform
- Group and broadcast communication for coordinated response
- Priority and pre-emption mechanisms for critical communications
- Interoperability with legacy communication systems
- High reliability and resilience for mission-critical environments
- Global standards compliance (3GPP)
- Secure communication with strong authentication and encryption
- Location-based services for enhanced situational awareness

4. Objectives

- Enable secure, real-time, and reliable communication for public safety agencies
- Enhance coordination and operational efficiency among first responders
- Support advanced situational awareness through integrated data and video services
- Modernize public safety communication infrastructure using broadband technologies
- Strengthen international cooperation in mission critical communication systems

5. Use Cases

C-DOT's MCX solutions can be deployed across diverse operational scenarios and geographies. Key use cases include:

- Public safety operations: Real-time coordination among police, fire, and medical services
- Disaster response: Multi-agency communication during natural disasters and emergencies
- Urban security: Surveillance integration and rapid response in smart cities
- Defence and border security: Secure and reliable communication in critical operations
- Transportation and critical infrastructure: Communication for railways, airports, and utilities
- Large public events: Crowd management and emergency coordination

6. Way Forward

C-DOT's Mission Critical Communication platform represents a significant step toward modernizing public safety communication systems through indigenous, standards-based innovation. Building on India's advancements, there is strong potential to expand international collaboration for deployment and adoption of MCX solution.

Digital Intelligence Platform (DIP)

1. Introduction

The **Digital Intelligence Platform (DIP)** is an indigenous citizen-centric solution developed to strengthen digital trust and combat various kinds of fraud including cyber frauds that are committed using telecom resources like Mobile SIM . It empowers users to monitor mobile connections issued in their name, report fraudulent activity, and block unauthorized services. DIP integrates telecom operators, financial institutions, and digital service providers on a common platform, enabling swift action against fraud, spam, and identity misuse. Successfully implemented in India, DIP represents a scalable and effective model for safeguarding digital communications.

2. Product Overview

DIP provides a unified interface for citizens to verify, manage, and secure their mobile connections, while also enabling regulatory and business stakeholders to coordinate remedial actions.

Key Highlights

- Citizens can check all mobile connections issued in their name.
- Facility to request disconnection of unauthorized or fraudulently obtained connections.
- Reporting of suspected fraud communications and spam (Unsolicited Commercial Communication).
- Provides certified details of customer care numbers, branch names, and official contact details of financial institutions.
- Backend integration with TSPs, financial institutions, and social media platforms for coordinated response.
- Facilitates sharing of deactivated numbers with businesses and apps that rely on mobile authentication.

3. Unique Strengths and Benefits

- **Citizen Empowerment:** Transparency in mobile connections and easy reporting mechanisms.
- **Fraud Prevention:** Detects and disconnects unauthorized mobile numbers.
- **Spam Control:** Mitigates UCC and phishing attempts.
- **Trustworthy Information:** Provides verified financial institution details to prevent scams.
- **Collaborative Ecosystem:** Connects TSPs, banks, and digital platforms for unified action.
- **Business Support:** Shares deactivated numbers to prevent misuse in banking, messaging, and authentication.

4. Objectives

- Protect citizens from identity theft, telecom fraud, and spam.
- Build a trusted digital ecosystem by validating customer care and service contact details.
- Enable swift, coordinated action across telecom operators, banks, and digital service providers.
- Strengthen national security and consumer protection through proactive fraud detection.

5. Use Cases

- **Consumer Protection:** Blocking fraudulently obtained SIMs and unauthorized connections.
- **Spam & Fraud Reporting:** Citizens report suspicious calls, SMS, or phishing attempts.
- **Financial Security:** Verified customer care numbers prevent financial scams.
- **Enterprise Enablement:** Banks, OTT platforms, and social media apps rely on DIP data for customer authentication.
- **Law Enforcement Support:** Facilitates faster investigation of telecom-related fraud.

6. Way Forward

- Enable international collaboration for cross-border fraud management.
- Extend DIP as a model for global adoption in countries facing rising telecom related cybercrime.