FORM 1

CCRP SCHEME APPLICATION REQUEST FORM

APPLICANT PROFILE

Applicant Name		**Santosh kumar Singh**
Designation		**Director & CTO**
Department		**Software Development**
Phone Number (Mobile No.)		**+91 8210613948**
Phone Number (Landline, if any)	STD code	Local code
Email		**saantoshs0293@gmail.com, info@advisionslab.com**
Last Educational Qualification		**M.Tech**
Institute of Last educational qualification		**National Institute of Technology Uttarakhand**

COMPANY PROFILE

Company Name of Primary Applicant		**Advisions Research and Development Private Limited**
Address (Head Office) of Primary Applicant	(Address line 1, 2) state code, pin code	**Gayatri Enclave, Under flyover NH58, Manglour, Roorkee, Haridwar - 247656, Uttarakhand, India**
TAN/PAN/CIN of Primary Applicant		**PAN: AAXCA7784M, CIN: U72900UR2022PTC014746**
Company Type (Checklist)		
	Startup (Default Value)	**Startup , MSME**
	MSME	
	Government Insttitution	
	Academia	
	PSU	
	Society	
	OTHER	Details (if OTHER)
Domestic	Yes/No	**Yes**
Registered	Yes/No	**Yes**
Size (Employee Strength)	(Head Count of company)	**12**
Company Area of work/Domain Expertise **Software Development**		
Company Turnover (last 3 years)		**14 lakhs**
Branches	Yes/No	**No**
Branch Details (Only if 'Yes' in Branches)		
	Branch1 Details	
	Address	
	Size (n:Head count of Branch)	
	Phone No.	
	Branch (n) Details	
	Address	
	Size (n:Head count of Branch)	
	Phone No.	

SOLE-APPLICANT/ CONSORTIUM DETAILS

Submitted By	Sole-Applicant / In-collaboration

Collaborator Details (Only of **"In-collaboration"** in "Submitted By" field)

Sr No.	Collaborator Organization Name	Company Address	Collaborator Type	Contact Person	Mobile No. of Point of contact	Domestic (Yes/No)	TRL level of participating product	Upload MoU (Yes/ No)
1	IIT Kanpur	Kalyanpur Kanpur -208 016	consortium partner	Angshuman Karmakar	+91 8967827714	Yes	1-9	Yes
2.	Advisions Research and Development Private Limited	Gayatri Enclave, Under flyover NH58, Manglour, Roorkee, Haridwar - 247656, Uttarakhand, India	consortium partner	Santosh Kumar Singh	+91 8210613948	Yes	1-9	Yes

PROPOSAL /IDEA DETAILS

Type of Proposed Solution (Mention only one of the suggested dropdown)	Product (Hardware + Software)	**Software**
	Idea	
	Software	
	Hardware	

TRL Level (1-5)

Area Of Technology of Proposed solution (mention only **ONE TECH AREA** name code from the suggested Dropdown)

TECH AREA Name	**Code (XXXX)**	
5G/6G Technologies	**5G6G**	**QKDC**
IoT and M2M Solutions	**IOTM**	
Artificial Intelligence, and Cognitive Sciences	**AIML**	
Telecom Network and Cyber Security	**TSEC**	
Radio, Wi-Fi, Satellite and Broadcast	**SRAN**	
Optical Access & Transport technologies	**OPTL**	
Network Management System and Framework	**NMGT**	
Advanced Telecom Applications	**APPN**	
SOC/Micro-system level Design	**MSOC**	
Quantum Communication	**QKDC**	
Transport Technologies(Routers, Switches, Aggregators)	**TSPT**	
Other	**OTHR**	Details (if Other)

Problem Statement in Focus

Development of Automated Tool (combination of black box tester and security scanner agent on the target device itself) to scan target device for discovery of generic security vulnerabilities and Quantum-vulnerable cryptographic algorithms.

Problem Statement (in case of suo moto)

Problem statement in 100 words

Problem Id of Problem Area in Focus

EOI-CCRP-QSC-psid-v02 (Post Quantum Cryptography (PQC), Vulnerability Assessment)

Proposed Solution

The Q-SecureScan project proposes an AI-powered tool designed to detect cryptographic algorithms and security protocols vulnerable to quantum computing attacks, enabling organizations to transition to post-quantum cryptography (PQC). This solution scans devices for quantum-vulnerable cryptographic schemes and common security weaknesses, using advanced algorithms to identify potential threats. It generates comprehensive reports with actionable insights, suggesting quantum-safe alternatives to replace at-risk protocols. With a modular design, user-friendly web interface, and real-time AI feedback, Q-SecureScan provides organizations with a proactive approach to safeguard their systems against quantum threats, ensuring compliance with future security standards and a seamless migration to PQC solutions.

Technical Feasibility

The technical feasibility of Q-SecureScan relies on proven cryptographic analysis methods, AI-driven vulnerability detection, and emerging post-quantum cryptographic (PQC) standards. The tool's development roadmap includes multi-phase technology validation, starting with research and proof-of-concept testing on common cryptographic libraries and security protocols. Through controlled lab testing, simulated pilot environments, and real-world operational trials, Q-SecureScan will refine its detection accuracy and system compatibility. Pilot readiness is targeted within six months, with a scalable deployment roadmap. IIT Kanpur leads the quantum research component, while Advisions manages the AI-based detection engine and implementation, ensuring robust validation and timely transition to full-scale deployment.

Innovative/Novelty Feature of Product/Idea

Q-SecureScan introduces a novel approach to cybersecurity by focusing on preemptively addressing quantum vulnerabilities, a future-proofing imperative as quantum computing evolves. Unlike conventional vulnerability scanners, Q-SecureScan integrates an AI-powered detection engine specifically designed to identify cryptographic schemes and protocols susceptible to quantum-based attacks. The tool uniquely combines standard security assessments with quantum-specific analysis, providing a dual-layered defense strategy. Leveraging Shor's and Grover's algorithm principles, it identifies weaknesses in algorithms like RSA and AES, pinpointing where current cryptography will falter against quantum threats.

A standout innovation is its modular architecture, which supports adaptive learning and scalability. The AI engine continuously refines its detection capabilities based on emerging cryptographic threats, while the modular framework allows seamless updates as new quantum-safe standards evolve. Another distinctive feature is its comprehensive reporting system, which not only highlights vulnerabilities but also suggests quantum-safe alternatives with a prioritized migration roadmap, tailored to each organization's specific environment.

Q-SecureScan's user-friendly web interface enables both black-box and authenticated scanning, ensuring accessibility for various industries. This proactive, AI-driven approach positions Q-SecureScan as a transformative tool, bridging today's cybersecurity standards with the quantum-secure future, empowering organizations to address both present and emerging digital threats.

Impact/Benfits of Proposed Solution

Q-SecureScan offers substantial benefits for industries like finance, defense, and healthcare by proactively addressing quantum vulnerabilities. With the quantum-safe cryptography market projected to grow significantly, Q-SecureScan meets critical demand for secure transitions. Its AI-driven, scalable solution positions organizations to safeguard sensitive data, ensuring future-proof compliance and robust digital resilience.

End-to-end solution

Q-SecureScan provides a comprehensive, end-to-end solution, seamlessly integrating AI-driven quantum vulnerability detection with traditional security assessments. Designed for diverse industries, it offers a scalable approach to identifying and replacing quantum-vulnerable algorithms, minimizing risk across cryptographic libraries, security protocols, and system configurations. The tool's centralized control dashboard supports deployment, monitoring, and report generation, ensuring that organizations can manage both current security vulnerabilities and quantum threats in a single interface. This integration enables organizations to transition confidently to quantum-safe standards, while its modular, adaptive design ensures that as quantum threats evolve, Q-SecureScan remains a reliable, updatable defense solution.

Cybersecure

Q-SecureScan is built with cybersecurity at its core, incorporating advanced, AI-driven detection of both traditional and quantum-specific vulnerabilities. It employs stringent security protocols, such as multi-layered encryption for data handling, secure access controls, and isolated data storage to protect sensitive scan results. The tool's web application includes secure login and authorization processes, minimizing unauthorized access risks. Furthermore, Q-SecureScan undergoes regular internal audits, vulnerability testing, and is designed with modular updates to quickly address emerging cyber threats. This approach ensures that Q-SecureScan itself remains secure and resilient, maintaining high standards for data integrity and confidentiality throughout its operational lifecycle.

Commercialization Strategy

The commercialization strategy for Q-SecureScan is rooted in providing a cutting-edge, quantum-safe cybersecurity solution tailored for industries at high risk of future quantum attacks, such as government, defense, finance, and healthcare. Developed in collaboration with IIT Kanpur and CDOT, this tool will leverage CDOT's national network and infrastructure to position itself as a trusted cybersecurity asset, ensuring adoption across sectors requiring compliance with stringent security regulations.

Q-SecureScan's AI-powered detection and easy-to-use interface deliver high value by automating vulnerability detection and migration to post-quantum cryptography (PQC), empowering organizations to preemptively secure sensitive data. The go-to-market strategy includes an initial pilot rollout with government entities via CDOT's network to validate the tool in high-security environments, followed by phased scaling to commercial and private sectors.

The tool addresses critical challenges like the complexity of identifying quantum-vulnerable protocols, the high cost and labor intensity of manual vulnerability assessment, and the urgent need for post-quantum migration support. By positioning Q-SecureScan as a proactive, scalable solution, the strategy aligns with CDOT's mandate to strengthen national cybersecurity defenses, ultimately driving wide adoption and establishing Q-SecureScan as the go-to quantum-safe cybersecurity solution.

Team The Q-SecureScan project will engage a team of over 15 experts, combining extensive technical and business expertise from IIT Kanpur, CDOT, and Advisions Research and Development. Leading cryptographers and quantum computing researchers from IIT Kanpur will focus on developing the core detection algorithms, ensuring quantum resilience. CDOT's cybersecurity specialists will oversee compliance, secure deployment strategies, and integration with government standards, leveraging CDOT's infrastructure to optimize Q-SecureScan's application for high-security environments. Advisions will provide software development, AI-driven vulnerability detection expertise, and business acumen to ensure the tool is user-friendly, scalable, and ready for commercial adoption. This cohesive team of experts will ensure the project's technical rigor, security, and market viability.

Expected Fund Requirement (Rupees In lakhs) (Also mention in words) **16240000 (one crore sixty two lakh forty thousand Rupees and zero paisa only)**

Expected Time for Delivery of Complete solution (In years) 1 year

Expected Customers/Clients Government, Finance, Healthcare, Defense, Corporates

Confirmation

1. Has the company been blacklisted/debarred by any agency/state government/central govrnment authority for any issues?

Yes/No **No**

Declaration

1. I, hereby, certify that all the facts/information/details provided above are true and correct to the best of my knowledge.

Digital Signature SANTOSH KUMAR SINGH

Digitally signed by SANTOSH KUMAR SINGH
Date: 2024.10.29 16:41:03 +05'30'

DOCUMENTS UPLOAD

Please Upload following documents:

Document Description	**Upload Status**	**Document Name As per specified format** (where XXXX is the technology Area code as specified above, NNN is Problem Id as given earlier in the form)
1. Organization Registration Document	Yes/No	CCRP-XXXX-NNN-Registration.pdf
2. Proof of being an Indian/Domestic Company	Yes/No	CCRP-XXXX-NNN-PIO.pdf (**P**roof of **I**ndian **O**rigin)
3. Write up on Product/Idea including mention of IPR	Yes/No	CCRP-XXXX-NNN-ProposalWriteup.pdf
Please structure your write up with separate sections for Objective, Problem Statement, Problem-Id, Technology, Technical Feasibillity, End-to-end Solution, Impact/ Use-cases, Background IP/Patents/Awards/Copyrights/Papers, Standard Body Contributions related to proposed solution/technology area, StandardCompliances, Awarded Certifications, Novelty, CyberSecure features, Commercialization strategy, Team Size and expertise, and how this is going to help individual/Organization/or industry		
4. Busienss presentation	Yes/No	CCRP-XXXX-NNN-BusinessPresentation.pdf
5. Uploaded MOUs (In case of submission in collaboration) - Collaborator 1	Yes/No	CCRP-XXXX-NNN-MoU1-PrincipalComapnyName-Collaborator1Name.pdf
6. Uploaded MOUs (In case of submission in collaboration) - Collaborator (n)	Yes/No	CCRP-XXXX-NNN-MoU(n)-PrincipalComapnyName-Collaborator(n)Name.pdf