Terms of reference (ToRs)

Third party security audit of KUSUM state portals (Phase II)	Project number/ cost centre: 16.2081.4-001.00

0. List of abbreviations 2

1. Context 3

2. Tasks to be performed by the contractor 4

3. Concept 6
Technical-methodological concept 6
Project management of the contractor 7

4. Company Profile 8

5. Personnel concept 8
Team leader cum Project Manager 8
Short-term expert pool with 5 9

6. Costing requirements 10
Assignment of personnel 10
Other costs 10

7. Inputs of GIZ or other actors 10

8. Requirements on the format of the bid 10

0. List of abbreviations

AVB	General Terms and Conditions of Contract (AVB) for supplying services and work 2018
ToRs	Terms of reference

1. Context

The Promotion of Solar Water Pumps (PSWP) component of the Indo-German Energy Programme (IGEN) is a bilateral technical co-operation measure between the Federal Ministry for Economic Co-operation and Development (BMZ), Germany and the Ministry of New and Renewable Energy (MNRE), Government of India. BMZ has commissioned Gesellschaft für Internationale Zusammenarbeit GmbH (GIZ), a federal enterprise based in Eschborn and Bonn in Germany, with the implementation of the project.

The PSWP module aims to improve, expand and speed-up the roll-out of sustainable solar water pumps. It is being implemented pan-India with focus to the East and North-East of India (specifically the federal states of Assam, Bihar, Jharkhand, and West Bengal), over a period of four years (October 2018–September 2022).

The objective is to ensure that solar pumps for productive use are rolled out more rapidly through a multi-level and multi-actor approach. The project provides advisory services to the central government (such as MNRE) at national level. In the selected federal states, it actively involves relevant government agencies (such as state implementing agencies), agricultural extension services and financial service providers. The project also accounts for the key role played by the private sector (companies and associations) by entering in specific cooperation arrangements.

The project will engage in four specific fields of activity: (i) promotion enabling policy environment,(ii) implementing successful business, operator and service models, (iii) facilitating access to finance and (iv) capacity building of agricultural service providers.

SWPs are steadily gaining ground in response to the subsidy support being provided under various central and state government schemes. New grid connected SWP models are also being promoted to enable additional farmer income through sale of surplus solar power generated by these pumps. The deployment is expected to increase multi-fold with the roll-out of MNRE's Pradhan Mantri Kisan Urja Suraksha Evam Utthan Mahabhiyan (PM KUSUM) which has three components targeting both on and off grid solar pumping as the following

Component-A: Setting up of 10,000 MW of Decentralized Ground/ Stilt Mounted Grid Connected Solar or other Renewable Energy based Power Plants;

Component-B: Installation of 2 million Stand-alone Solar Agriculture Pumps; and

Component-C: Solarisation of 1.5 million Grid Connected Agriculture Pumps

Given the importance of the scheme, MNRE is in the process of developing a dedicated and comprehensive national and state portal that undertake the massive task of monitoring implementation of PM KUSUM and the performance of pumps installed under the scheme. A key output for the PSWP module is to support development of a monitoring system that supplies MNRE and other stakeholders with information on the effectiveness of the promotion programmes and possible environmental impacts especially focusing on groundwater. Thus, the PSWP team is providing technical support to the MNRE in developing the PM KUSUM national and state portals.

MNRE, with support from GIZ, is developing state-level portals and integrating that with National Portal for monitoring progress of PM KUSUM in phased manner. In Phase-II, state portals are being developed in 13 states.

Given this background, the objective of this ToR is to carry out third party security audit of the web-portals for monitoring of all three (A, B & C) components of PM KUSUM scheme.

2. Tasks to be performed by the contractor

The scope of work for the contractor broadly corresponds to carry out third party security audit of state-level Solar Energy Data Management (SEDM) software platform for monitoring of PM KUSUM scheme Components (A, B and C) in various states as detailed in **Annexure I**. The SEDM software platform being developed cover both the parts as per MNRE guidelines where Part-1 is related to System Related Business Modules such as Application Pre Processing, Consumer Management, Site Survey Mobile Application, Asset Management, Scheme Progress Management, Live Asset Monitoring Dash Board, Performance Dash Board, MIS Dash board and Reports, Complaint & Ticket Management etc. and Part-2 is related to RMS Device Integration related SCADA modules such as Device Management with Security, SCADA Tag Processing, Alarm/Events & Notification Processing, Database Archiving and Historian, MDAS/MDM, Report Manager etc. Details of the same is as indicated in the "Technical Specifications" document.

The development of portals for the respective states and components have been already started and the security audit for the same need to be carried out as and when the development work is completed and ready for security audit within the project duration. As none of the portal ready, the shared technical details of the portal (based on previous experience) in **Annexure II** may be considered as tentative, but close to realistic. There may be change of around ±25 % depending on the customization request from the states. Bidder may consider this variation of scope of work in their bid.

The information security audit is to be conducted for web application, Web API and mobile applications ion developed in accordance with the guidelines of Cert-in Govt. of India, NICSI and OWASP. The tasks to be carried out includes the following.

a. Evaluation of web application, Web API and mobile applications configuration and testing reporting of gaps/ vulnerabilities/improvements (if any) and provides suggestions for solutions/mitigating strategies to tackle the same.
b. To test the resilience level of web facing interfaces by conducting audit as per latest OWASP (Open Web Application Security Project) attack guidelines and Vulnerability Assessment and Penetration Testing. The objective of the assessment is to determine the ability to withstand an intrusion attempt. This may be achieved by conducting both reconnaissance and a comprehensive penetration test. The security assessment should use the industry standard penetration test methodologies (like OSSTMM) and scanning techniques and will focus on web application, Web API and mobile applications. The application tests should cover but not limited to OWASP Top 10 attacks.

c. Documentation of the security gaps i.e. vulnerability, security flaws, loopholes, etc. observed during the course of the review of web portal. Documentation of recommendations for addressing these security gaps and categorization of identified security gaps based on their criticality.
d. The Information Security Audit Firm will conduct the Information Security Audit on the web application, Web API and mobile applications updated by the portal developers incorporating the suggestions provided by audit firm till it compliances with the information security audit requirements. Based on the compliance of web application, Web API and mobile applications, the ISA firm will issue Security Audit certificate for the web portal.
e. At least two iterations of security audits to be conducted on web portal, API and mobile application till identified safe for hosting and issue of security audit certificate.
f. The firm should provide support to the development team for changes in coding to remove vulnerability, if required.
g. The web application and API would be hoisted in separate URLs for each state. The Information Security Audit need to be carried out accordingly.
h. The firm need to ensure that security audit report and certificate are accepted by the provider of server to host the SEDM software in each selected state.

Black Box testing for Security Audit should follow OWASP (Open Web Application Security Project) guidelines covering but not limited to the following :

a) Cross-site scripting (XSS)
b) Injection flaws, particularly, SQL injection. Also consider LDAP and Xpath injection flaws as well as other injection flaws
c) Input validation flaws
d) Malicious file execution
e) Insecure direct object references
f) Cross-site request forgery (CSRF)
g) Information leakage and improper error handling
h) Broken authentication and session management
i) Insecure cryptographic storage
j) Insecure communications
k) Failure to restrict URL access
l) Denial of service.

Deliverables

Given the objectives and tasks listed above, the contractor is expected to deliver the following for each of the components of different states:

a. Vulnerability Assessment and Analysis Report for each iteration for each component as applicable to the State
b. Information Security Audit report for each component as applicable to the State
c. Information Security Audit Certificate for each component as applicable to the State

Timeline

Certain milestones, as laid out in the table below, are to be achieved by certain dates during the contract term:

Milestone	Deadline
Inception meeting and submit strategy after consultation with GIZ and portal developer	4th week
Submission of Vulnerability Assessment and Analysis Report for each component of the respective State	Within one week of indent/revisions
Submission of Final Audit report with information security audit certificate for each component of the respective State	Within one week of final revision

Period of assignment: 8 months from the date of the contract (from August 2021 until March 2022)

An inception meeting after the contract is accepted as well as monthly meetings or update calls (including minutes of the meetings between 2-3 pages) are mandatory. In the inception meeting, the contractor is required to give a presentation on the approach, methodology, details on schedule and milestone and discuss the assignment with GIZ. Furthermore, GIZ will provide a project monitoring sheet to the contractor. The contractor is responsible to fill in the sheet and send an updated version at the end of each month to GIZ.

3. Concept

In the bid, the bidder is required to show how the objectives defined in Chapter 0 are to be achieved, if applicable under consideration of further specific method-related requirements (technical-methodological concept). In addition, the bidder must describe the project management system for service provision.

Technical-methodological concept

Strategy: The bidder is required to consider the tasks to be performed with reference to the objectives of the services put out to tender (see Chapter 1). Following this, the bidder presents and justifies the strategy with which it intends to provide the services for which it is responsible (see Chapter 0).

As a part of the strategy description, the bidder is expected to provide concise answers to the following questions

- **What would be your strategy for carrying out this assignment to enable various components (of PM KUSUM) of States to be made safe to host in minimum time.**
- **Which major vulnerabilities/security risks do you foresee in developing this kind of web application, Web API and mobile applications? How do you minimise no. of iterations carried out to conduct information security audits?**
- **Which software tools do you use for conducting information security audits?**

- **Do you use manual process in security audits? If yes, please elaborate.**
- **Which standards/guidelines do you follow in conducting information security audits of web application, Web API and mobile applications?**

The bidder is required to present the actors relevant for the services for which it is responsible and describe the **cooperation** with them.

The bidder is required to present and explain its approach to **steering** the measures with the project partners and its contribution to the results-based monitoring system.

The bidder is required to describe the key **processes** for the services for which it is responsible and create a schedule that describes how the services according to Chapter 0 are to be provided. In particular, the bidder is required to describe the necessary work steps and, if applicable, take account of the milestones and contributions of other actors in accordance with Chapter 0.

The bidder is required to describe its contribution to knowledge management for the partner and GIZ and promote scaling-up effects (**learning and innovation**).

Project management of the contractor

The bidder is required to explain its approach for coordination with the GIZ project.

- The contractor is responsible for selecting, preparing, training and steering the experts (international and national, short and long term) assigned to perform the advisory tasks.
- The contractor makes available equipment and supplies (consumables) and assumes the associated operating and administrative costs.
- The contractor manages costs and expenditures, accounting processes and invoicing in line with the requirements of GIZ.
  The contractor reports regularly to GIZ in accordance with the GTCC of the Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ) GmbH from 2017

The bidder is required to draw up a **personnel assignment plan** with explanatory notes that lists all the experts proposed in the bid; the plan includes information on assignment dates (duration and expert days) and locations of the individual members of the team complete with the allocation of work steps as set out in the schedule.

The bidder is required to describe its backstopping concept. The following services are part of the standard backstopping package, which (like ancillary personnel costs) must be factored into the fee schedules of the staff listed in the bid in accordance with section 10.2 of the GTCC:

- Service-delivery control
- Managing adaptations to changing conditions
- Ensuring the flow of information between GIZ and field staff
- Contractor’s responsibility for seconded personnel
- Process-oriented technical-conceptual steering of the consultancy inputs
- Securing the administrative conclusion of the project

- Ensuring compliance with reporting requirements
- Sharing the lessons learned by the contractor and leveraging the value of lessons learned on site

4. Company Profile

Commercial Eligibility Assessment

· Please provide the legal status of your firm.

· Average annual turnover of the agency for the last three financial years: at least Euro 35000.

· The number of employees of the agency as at 31.12. of the previous year: at least 5 persons.

Technical Eligibility Assessment

The bidder shall have reference projects with a minimum commission value of 2000 EUR:

· 5 reference projects in the technical field of information security audit

· 3 reference projects in India in the last 3 year

. The Bidder must be empanelled with CERT-In as Information Security Audit Organization at the time of bidding and during the concurrency of this project

. The Bidder firms should not have been blacklisted/ debarred by any Government / Semi Government Departments/ PSUs / in India during last 3 years and Blacklisting should not be in force

Technical Experience

· Minimum 5 years of experience in national or international projects for information security audit of web portal and mobile applications

· Minimum 4 years of experience in Information Security/Cyber Security Audit in Govt. organisation/PSUs in India.

5. Personnel concept

The bidder is required to provide personnel who are suited to filling the positions described, on the basis of their CVs (see Chapter 8), the range of tasks involved and the required qualifications.

The below specified qualifications represent the requirements to reach the maximum number of points.

Team leader cum Project Manager

<u>Tasks of the team leader</u>

- Overall responsibility for the advisory package of the contractor
- Coordinating and ensuring communication with GIZ, partners and others involved in the project

- Personnel management, in particular identifying the need for short-term assignments within the available budget, as well as planning and steering assignments and supporting local and international short-term experts
- Ensuring results monitoring is conducted
- Regular reporting in accordance with deadlines
- Supporting the officer responsible for the commission in updating/adapting the project strategy, in evaluations and in preparing a follow-on phase

Qualifications of the team leader

- Education/training (2.1.1): Information Security related qualifications (CISSP/ISMS LA / CISM/ CISA/ ISA and equivalent)
- Language (2.1.2): Good business language skills in English and Hindi
- General professional experience (2.1.3): 8 years of professional experience of information system security
- Specific professional experience (2.1.4): 5 years in professional experience in conducting information security audits for Govt organisations and PSUs.
- Leadership/management experience (2.1.5): 5 years of management/leadership experience as project team leader or manager in a company
- Regional experience (2.1.6): 5 years of experience in information security audits in India
- Development Cooperation (DC) experience (2.1.7): 2 years of experience in DC projects
- Other (2.1.8): Experience of RE project will be an advantage

In addition to the above position, the bidder shall submit a pool of short-term experts as follows:

Short-term expert pool with 5

Tasks of the short-term expert pool

- Carry out the security audit of the portals and mobile applications
- support to the development team for changes in coding to minimise vulnerability
- Suggest corrective action and steps to remove identified vulnerability

Qualifications of the short-term expert pool

- Education/training (2.2.1): Information Security related qualifications (CISSP/ISMS LA /CISM/ CISA/ ISA or equivalent)/ M.Tech (cyber security/information security)/CEH/CSA or equivalent)
- Language (2.2.2): Good business language skills in English and Hindi
- General professional experience (2.2.3): 4 years of professional experience in information system security
- Specific professional experience (2.2.4): 3 years' experience in conducting information security audits for Govt organisations and PSUs.
- Other (2.2.7): Experience of RE project will be an advantage

Soft skills of team members

In addition to their specialist qualifications, the following qualifications are required of team members:

- Team skills
- Communication skills
- Efficient, partner- and client-focused working methods
- Interdisciplinary thinking

The bidder must provide a clear overview of all proposed short-term experts and their individual qualifications.

6. Costing requirements

Assignment of personnel

The assessment of the required human days for each state for the listed tasks is as follows:

Personnel	Number of expert days
Team Leader cum Project Manager	60 days
Short-term expert pool (security auditors)	240 days
Total expert days	**300 days**

Travel

The bidder is required to calculate the travel by the specified experts and the experts it has proposed based on the places of performance stipulated in Chapter 0 and list the expenses separately by daily allowance, accommodation expenses, flight costs and other travel expenses.

Other costs

- Please specify any additional costs

Contractor is required to submit activity-wise costing in their proposal.

7. Inputs of GIZ or other actors

GIZ shall help in steering the study along with the implementation partners.

8. Requirements on the format of the bid

The structure of the bid must correspond to the structure of the ToRs. In particular, the detailed structure of the concept (Chapter 3) is to be organised in accordance with the positively weighted criteria in the assessment grid (not with zero). It must be legible (font size 11 or larger) and clearly formulated. The bid must be drawn up in English (language).

The complete bid shall not exceed 10 pages (excluding CVs and company experience).

The CVs of the personnel proposed in accordance with Chapter 4 of the ToRs. The CVs shall not exceed 4 pages. The CVs must clearly show the position and job the proposed person held in the reference project and for how long. The CVs should also be submitted in English.

If one of the maximum page lengths is exceeded, the content appearing after the cut-off point will not be included in the assessment.

Please calculate your price bid based exactly on the aforementioned costing requirements. In the contract the contractor has no claim to fully exhaust the days/travel/workshops/ budgets. The number of days/travel/workshops and the budget amount shall be agreed in the contract as ‘up to’ amounts. The specifications for pricing are defined in the price schedule.

The shortlisted candidates may be invited for a presentation in either in virtual platform (most probably) or in GIZ Delhi Office within 45 days of the submission of the proposal.

Annexure-I

Specific Conditions pertain to Covid- 19 Measures

The specific conditions pertain to Covid- 19 measures are integral part of contract and shall act as binding document under special agreement and interpreted along with GTCC.

In addition to the provisions as detailed in clause 09 of The General Terms of Contract governing the delivery of works and services commissioned by Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ) GmbH (local), the Consultant confirms that he/she accepts the Consulting engagement with full knowledge and understanding of the travel and other requirements of the engagement including specifically the need, on the part of the Consultant, to take all required precautions (including prevention and risk mitigation measures) against the risks arising from the ongoing Novel Corona Virus (CoVid - 19) Pandemic.

The Consultant shall provide to the GIZ an RT-PCR Negative Test Report for Novel Corona Virus (CoVid - 19) prior to starting the Consulting Engagement and shall additionally comply with the following at all times in the course of the Consulting Engagement:

1. Obtain Medical and other Insurance Cover in respect of the Novel Corona Virus (CoVid - 19) Infection/Disease and consequences thereof – (GIZ will reimburse the insurance cover up to 5000 Indian Rupees)

2. Strictly follow and comply with the prescribed Mask, Hand Washing/Sanitization and Social Distancing Protocols.

3. Take safe and secure mode of transportation.

4. Observe all local restrictions/precautions as applicable for the specific areas of travel covered by the Consulting Engagement.

5. If eligible, get vaccinated against the Novel Corona Virus (CoVid - 19).

6. Install and maintain as active at all times the Government of India's Arogya Setu App.

7. If exposed to any active case of Novel Corona Virus (CoVid - 19) to take all steps as advised by the Government of India's advisories in such case.

8. If feeling unwell and experiencing any of the symptoms of Novel Corona Virus (CoVid - 19) infection - to take all steps as advised by the Government of India's advisories in such cases including but not limited to getting an RT-PCR Test for Novel Corona Virus

(CoVid - 19), selfisolation, notifying the GIZ and also the concerned local Novel Corona Virus (CoVid - 19) isolation/treatment facility.

9. Other compliance as may be notified by the GIZ and the Government of India from time to time in relation to Novel Corona Virus (CoVid - 19) infection/disease.

Furthermore, The Consultant accepts the Consulting Engagement on a best and informed judgement basis with full knowledge of the tasks to be performed, the place of performance and the precautions and safeguards to be reasonably taken by the Consultant to mitigate all types of risks associated with the said Consulting Engagement. The Consultant undertakes the Consulting Engagement at his/her own risk and responsibility and shall not, under any circumstances, and at any time, be entitled to assert any liability or other claims whatsoever against the GIZ, its Management, Officers and Employees for any consequences or risks or harm that may arise to the Consultant in the course of or as a consequence of undertaking the Consulting Engagement or any actions or consequences arising in relation to such Consulting Engagement.

Annexure II

State-wise Component-wise Portal Development Details

S. No.	State	Component selected for portal development		
		Component-A	Component-B	Component-C
1	Andhra Pradesh			√
2	Goa			√
3	Jammu & Kashmir		√	
4	Jharkhand		√	
5	Karnataka		√	√
6	Madhya Pradesh	√		√
7	Maharashtra			√
8	Odisha	√	√	
9	Punjab			√
10	Rajasthan	√		√
11	Tamil Nadu	√		√
12	Telangana	√		√
13	Uttar Pradesh	√		√
	Total	**6**	**4**	**10**

This is to be noted that SEDM platform is already developed/being developed for component B for the states of Rajasthan, Tamil Nadu, Uttar Pradesh and Punjab. Each state SEDM platform comprises of all three components of PM KUSUM and all three components are accessible from a single url.

Annexure-III

S.No.	Parameter	Description		
		Component A	Component B	Component C
Web Application				
1	Web Application Name & URL	Will be shared before start of the audit		
2	Operating System	Windows Server 2016 Data centre		
3	Application Server with Version	IIS 10		
4	Front-end Tool	Visual Studio Code, HTML, CSS, JS		
5	Back-end API Tool	Visual Studio 2017		
6	Back-end Database	MySQL 5.7.27		
7	Authorization no. of roles & types of privileges for the different roles	4	4	**4**
8	Content management module (CMS)	No	No	**No**
9	Number of forms & input fields	31	31	**31**
10	No. of login modules	3	3	**3**
11	Does the application provide a file download feature	yes	Yes	Yes
12	Provision of e-Commerce or Payment Gateway	No	No	No
13	Number of Roles in the application	4	4	4
14	Number of static pages	7	7	7
15	Number of Dynamic Pages	75	132	150
16	Payment Gateway Integrated with the application	No	No	No
17	Number of User Input fields (approximately)	200	380	400
18	Whether the web application contains any Content Management System. If yes, please mention name of the CMS	No	No	No
19	Are you maintaining application logs Yes/No	Yes	Yes	Yes
20	Willing to provide server remote connection to collect the log evidences	Yes	Yes	Yes
21	Will the website/web application/webservice available remotely for auditing	Yes	Yes	Yes
Web API				
23	Webservice URL	Will be shared before start of the audit		
24	Will the website/webapplication/webservice available remotely for auditing	Yes	Yes	Yes
25	Number of Roles in the application	4	4	4
26	Number of Methods	150	266	300

27	Type of Web service (Restful , SOAP etc.,)	Restful	Restful	Restful
28	Payment Gateway Integrated with the application	No	No	No
Mobile Application				
29	Type of Application, Native or Hybrid	Hybrid		
30	Supportive Operating System	Android		
31	Does the application has a login interface if so , how many user roles are available	Yes, 4 roles		
32	Number of Screens	58		
33	Number of Activities	95		
34	Number of User Input fields (approximately)	153		