Chhattisgarh Infotech Promotion Society | Government of Chhattisgarh

Integrated Proactive e-Governance (IPeG)

REQUEST FOR PROPOSAL FOR SELECTION OF MASTER SYSTEM INTEGRATOR

FOR

DESIGN, IMPLEMENTATION, OPERATIONS AND MAINTENANCE OF IPEG

(Vol. II – Terms of Reference)

Contents

Table of Figures

1. INTRODUCTION

1.1. Background

One of the core functions of the government is to deliver the public services to its citizens. The citizens have to comply with lengthy and repetitive documentation, make multiple physical visits, wait for the desired outcome without any assurance of timelines. On the other hand, government is also constrained with limited resources, conventional paper-based processes and lack of standardization across various government entities. Thus, the current state of public service delivery affects the citizens as well as the government.

The state government is committed to enhance the social safety net of people of the state. In addition to providing social benefits, government intends to provide timely and convenient delivery of public services and social benefits. Given the people-centric focus of the state government and the fact that the government engages lot of resources in the delivery of services and benefits to the state's nearly 3 crore people and technological advancements, it is imperative that a fresh look at transforming public service delivery be taken. With increased citizen expectations, the government is being asked to deliver the public services in a more convenient manner. In order to meet these expectations, the government intends to provide timely and convenient delivery of public services and social benefits and improve the efficiency of public service delivery.

The service delivery models, both public and private, have been disrupted worldwide by the use of data and technology, through which it is now possible to customize the delivery of service according to a person's preferences at an affordable cost. Several countries such as Estonia have transformed their public service delivery using data and technology. Even in India, the citizens have experienced certain public services (e.g. Passport, Aadhaar) and non-public services (e.g. telecom, banking) being delivered efficiently and in a hassle-free manner. The advent of national digital assets such as Aadhaar, Unified Payment, Interface, e-Sign, Digital Locker etc. has accelerated the pace of digitization and standardized some of the processes involved in delivery of services.

The elected Government of Chhattisgarh intends to enhance the social safety net of residents of the state. In addition to providing social benefits, government intends to provide timely and convenient delivery of public services and social benefits. Given the people-centric focus of the state government and the fact that the government engages the majority of its resources in the delivery of services and benefits to the state's 25 million people and technological advancements, it is imperative that a fresh look at transforming public service delivery be taken.

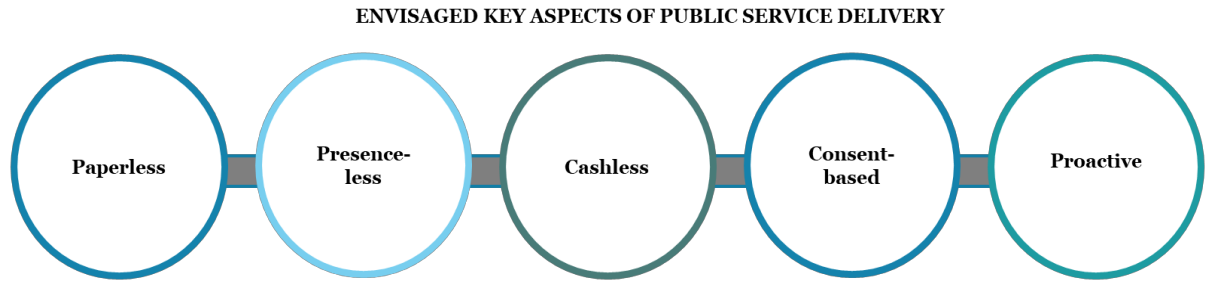
In line with the commitment made by the Government of Chhattisgarh and the expectations of the people, Chhattisgarh Infotech Promotion Society (CHiPS) has envisaged the Integrated Proactive e-Governance (IPeG) program with the twin objective of enhancing citizen experience while availing public services and improving the efficiency of public service in the state of Chhattisgarh. For detailed vision and objectives of the IPeG program.

1.2. Project Vision, Goals and Objectives

This section describes the envisioned stage across the service delivery and outlines the overall vision and objectives of IPeG program.

1.2.1. Project Vision

The broad vision of IPeG is a governance regime that is paperless, presence-less, cashless, consent-based and ensures proactive delivery of public services, giving utmost importance to effective grievance redressal.



Paperless – No need for citizens to submit paper documents / certificates

Presence-less – Physical presence of the citizen not required

Cashless – Provision to accept service charge electronically and 100% electronic transfer of monetary benefits

Consent-based – Citizens decide what to share, with whom to share and whether to opt for proactive service delivery

Proactive – Automatically register and deliver entitlements to citizens

Figure 1: Envisaged Key Aspects of Public Service Delivery

Chhattisgarh Infotech Promotion Society (CHiPS) has envisaged the Integrated Proactive e-Governance (IPeG) program to meet the above vision.

- **Paperless**: The program envisages that the citizen will be required to provide data elements (information and documents) only once to the government and these data elements will be used to deliver the services in a convenient manner initially and proactive manner subsequently. This will require departments to collaborate and re-utilize the data elements and documents in public service delivery i.e. there will an exchange of data element needed by one department (user department) for service delivery and owned by another department (owner department). As all the departments will rely on available data for service delivery, it is very important to maintain a high degree of accuracy. For each data element, the most trusted source of information will be identified and the concerned departments will have to ensure data element corresponds to correct individual through adoption of robust seeding protocol, and that data element is correct and up-to-date through citizen friendly, well-designed and time-bound processes for correction and update of data.

- **Presenceless**: The program will establish/utilize an ecosystem of shared infrastructure such as services portal, mobile application, door-steps delivery mechanism, service delivery outlets, call centre, etc. This will ensure that the presence of the resident is either not required or limited presence is required for service delivery.

- **Cashless**: The public service require the resident to make payment of nominal fees. Under IPeG, the resident should be able to make payment of this fees through multiple electronic means such debit card, credit card, wallet, UPI, etc. Moreover, the social protection schemes envision transfer of benefits into the beneficiaries' bank account.

- **Consent-based:** To deliver the public services, the resident's data will be captured, stored and processed under the IPeG program. The privacy of the resident will be one of the core elements of the program design. Thus, the data is envisioned to be captured, stored or processed as per the consent obtained from the citizen.

- **Proactive:** Upon citizen's consent for proactive service delivery, the resident should be able to avail public services and register in social protection schemes without the need to apply for them. To ensure the privacy of citizen data, a federated structure of data repository will be utilized wherein each data element will be stored by concerned trusted source.

1.2.2. Objectives

Integrated Proactive e-Governance (IPeG) program has been conceptualized by Government of Chhattisgarh to achieve the following objectives in relation to public services delivered using this program:

- enhancing citizen experience while availing public services, benefits and subsidies,
- improving efficiency in delivery of public services, benefits and subsidies,
- enabling evidence-based policy design and/or decision making
- addressing citizens' grievances by setting up a robust grievance redressal mechanism

This project, amongst other things, would help achieve the objectives for Result Area 4 (DLI#9) of the World Bank Program – Chhattisgarh Public Financial Management and Accountability Program.

The overall objective of the World Bank program is to improve accountability in the management of public finances; strengthen revenue administration; and improve efficiency in delivery of benefits in selected schemes, in the state of Chhattisgarh.

Key Result Area	Nodal Agency
Strengthening Core Financial Management Systems and Services	Finance Department
Strengthening Financial Management of Local Bodies	Chhattisgarh Urban Development Agency
Strengthening Revenue Administration	Commercial tax Department

Key Result Area	Nodal Agency
Improving efficiency in delivery of benefits in selected schemes	Chhattisgarh Infotech Promotion Society

The objective of Result Area 4, that shall be achieved through IPeG, is **"Universal Use of DBT for validated baseline of the beneficiaries in selected schemes".**

World bank is extending a loan of $25.2 Million for this program. Republic of India is the borrower and Finance Department, Government of Chhattisgarh is the Implementation Agency of the overall World Bank program. Out of the loan amount of USD 25.2 million, the amount earmarked for the Result Area 4 (DLI#9) is USD 10 million. CHiPS is the nodal agency for the Result Area 4 (DLI#9) of the program.

However, in addition to meeting the objectives of the World Bank program, IPeG also plans to cater to additional objectives of improving G2C service delivery in the state. Thus, it aims to transform the landscape of all possible interactions between the government and citizen.

1.3. Overview of current state and envisioned state of Government to Citizen Service Delivery in the state

Constitution of India enshrines it as a welfare state and plays a key role in the protection and promotion of the economic and social well-being of its citizens. As a result of this, all states and UTs in India follow this in letter and spirit. Promotion and protection of citizen wellbeing is operationalized through a wide range of public services which are offered by the different state and central government departments. Government of Chhattisgarh also offers multiple Government to Citizen services. These include welfare centric Direct Benefit Transfer services, regulatory services which help ensure rule of law, statutory services which a citizen is entitled through naturalization and consumer utility services such as water supply, electricity and other basic amenities. To ensure accountability of government and timely delivery of services, many of them are governed by Lok Sewa Guarantee Act 2011, which stipulates the exact timelines which need to be adhered to while delivering a service.

In spite of a legal backing to service delivery in the state and other concerted efforts of the state government, availing all categories of public services and benefits mentioned above is affected by various challenges such as cumbersome and repetitive processes for citizens, unassured timelines of service delivery for the citizens, governments' limited resources, etc.

The evolution in technology has enabled transformation in service delivery models in private as well as public sector across the world. In India, the effects of transformations are visible in passport, Aadhaar, telecom, banking, etc. The adoption of technology had led to creation of digital assets which acts as a catalyst in digitization of public services in the country.

The state government is committed to enhance the social safety net of people of the state. In addition to providing social benefits, government intends to provide timely and convenient delivery of public services and social benefits. Given the people-centric focus of the state government and

the fact that the government engages lot of resources in the delivery of services and benefits to the state's nearly 3 crore people and technological advancements, it is imperative that a fresh look at transforming public service delivery be taken.

As a part of our project, various schemes and their supporting services have been referred to as a **public service**, schemes (where a citizen gets a tangible benefit) have been referred to as the **core services** and the services which could be stand alone or help citizen in availing a core service have been referred to as **enabler services**. For e.g. BPL scholarship given out to students in the state would be a core service whereas the BPL certificate and Domicile certificate which student would need to avail this core service are what we refer to as the enabler service.

In this section major challenges across the lifecycle of service delivery of citizens have been highlighted and envisioned state of service delivery has been defined. The section has been outlined in accordance to following stages of lifecycle of public service delivery life cycle:

- Design and Launch of a scheme/service (Design and Launch)
- Application by citizen for the public service and approval of the same by Government official (Application and Approval)
- Benefit/Service Output disbursement
- Feedback and Grievance handling

1.3.1. Design and Launch

At present, most of the public services that are launched utilize the data that is dated. Moreover, sometimes decisions related to service design are based on popular perceptions and lack empirical evidence. The design parameters are also based on prior experience of administrators and are not always guided by decision support systems. Additionally, once a public service has been designed, launch takes considerable time as identifying the right set of beneficiaries or accurate targeting is a challenge in absence of reliable data sources and tools for performing analysis.

a) Problems from Citizen Perspective

The public services have two kinds of criteria i.e. inclusion criteria and exclusion criteria which are often set based on unreliable data. In case these criteria are not set correctly, it can lead to inclusion of unintended beneficiaries or exclusion of intended beneficiaries leading to inefficient utilization of public funds and eventually the socio-economic development of the citizens may get affected.

- **Exclusion Errors:** Citizen face issues in registering themselves due to exclusion errors wherein intended beneficiaries may be left out.
- **Inclusion Errors**: On the other hand, due to the inclusion errors there are challenges in benefits being delivered to the unintended residents.

b) Problems from Government Perspective

The design of a public service in the state is being carried out on the basis experience/understanding of policy makers/peoples' representatives of the needs of the residents

or the limited empirical evidence. At the time of design of new schemes/programs, it is difficult to estimate the approximate number of beneficiaries, the budgetary allocation required, the targeting of eligible beneficiaries, and operationalization time of the scheme. As of now, policy makers/administrators find it difficult to undertake simulation of different scenarios of scheme inclusion criteria, benefit amount per beneficiary and their impact on number of beneficiaries and total budget required. This inability to undertake simulations and not being able to estimate number of beneficiaries and budget amount makes it difficult for policy makers to design efficient schemes/programs.

The key reason behind above problems is that many government data sources in the state/country are outdated, inaccurate or incomplete. Additionally, there is lack of unified information resource across departments in the state that can give a macro-level view on basis of sectors, development indicators, geographies, demographic groups etc. This leads to the problem of sub-optimal resource allocations and in-effectiveness of schemes rationalization.

c) Envisioned state

The state intends to move towards a governance regime where data driven decision making is enabled i.e. all public services are designed and launched with the help of up-to-date and accurate data and with help of empirically driven decision support systems. Additionally, it intends to focus on both macro-and micro-factors of public service implementation, therefore there is a need for one stop monitoring platform for the services. This will not only enable better design of public services but also ensure speedy operationalization of public services designed and planned for launch.

The envisioned state for ‘Design and Launch’ stage of Government to Citizen service delivery can be summarized as:

- Data driven policy making and service design
- Real time monitoring of public services for adjustments and relaunch
- Rapid operationalization of public services designed and planned for launch

1.3.2. Application and Approval

The previous section explained about public service delivery and launch. After a public service is launched, the citizens need to apply for the same in order to avail the service benefits.

The state has taken efforts to make G2C services available online and at Service Delivery Centres (Lok Sewa Kendras (LSK), Common Service Centres (CSC) and CHOiCE centres) across the state e.g. e-District platform offers 126 services online. Out of these services, significant volumes of application are through Service Delivery Centres like LSK or CSC centres.

In addition to the above services, there are many public services which are being delivered either in an offline manner and online through department specific applications/portals. Till now, nearly 170 core services have been identified, benefits under which can be delivered to the citizens through Direct Benefit Transfer (DBT) mode. However, to apply for these services citizens need to conduct multiple visits to CSCs, LSKs and government offices. In case there are some problems with approval, getting to know the exact problem with approval gets difficult for citizen,

and this requires the citizen to visit the concerned location again. The problems are compounded with the need to carry paper copies of government issued certificates or supporting documents which need to be submitted repeatedly whenever a new application is made by the citizen.

From a government perspective, different departments are at different stages of IT enablement and thus approvals are contingent upon the level of IT enablement. Many services still require manual approvals, some are semi-digitized while few are digitized end-to-end. However, irrespective of the stage of IT enablement, some issues are consistent across approval mechanisms of all services. These include verifying validity of a scanned document, in absence of originals, verifying identity of applicant and the institution which they have affiliation to (if applicable). Also, another major challenge is maintaining transparency with the applicant with respect to status of approval and reasons for rejection/ return, wherever applicable.

a) Problems from Citizen Perspective

The citizens face multiple challenges in terms of current process of service application which are mentioned below:

- **Awareness (Existence)**: The citizens are not aware about the existence of entire set of services delivered by the government.

- **Awareness (Service Information)**: The citizens are not aware about eligibility conditions, documentation required for application, access channels, service fees, etc.

- **Access:** For residents staying in the State, the services are often available at the Tahsil or District headquarters whereas for residents staying outside state the services are accessible only within the state. In both cases, the citizens are required to travel to the specified location resulting in loss of time and wage.

- The accessibility of G2C services in the state is poor and owing to this, citizens find it difficult to access and apply for these services. Some of the major reasons for poor accessibility are as follows:
  a) Many G2C services are still offered only at Government offices situated at Tehsil/District Headquarters and not at Service Delivery Centres in Gram Panchayats/Urban Local Bodies. The current e-District application accessible across the Service Delivery Centres in the state does provide access to all the G2C services.
  b) As mentioned in the previous section, many core services are still offered in manual mode making it difficult to make it accessible at Service Delivery Centres.
  c) The penetration of Citizen Service Delivery Centres is not adequate especially in Southern and Norther parts of the state. Low business viability owing to availability of very few services especially for rural areas is one of the major contributing reasons behind low penetration of these centres.
  d) Applications to very few services can be made by citizens through their mobile apps, or web portals, or service delivery centres across the state

- **Pre-requisites**: In some cases, public services are provided on basis of pre-established national or state government database like SECC, BPL, etc. In case the citizen is not part of

these databases, the citizen either gets excluded or must apply separately to become part of such database.

- **Documentation:** To avail the public service, the citizen needs to provide relevant information and submit supporting documents at the time of application. The aforementioned information and documents asked from citizens is issued by the government itself but is still requested repeatedly from citizens whenever they apply for a public service. In absence of the supporting documentation, the application form gets rejected for want of documentation which government had issued itself and need not have asked in the first place.

  Many services require notarized/attested documents. This requires citizens to go to the required Government offices. Thus, a citizen is required to go to multiple offices to be able to apply for a service. This also defeats the purpose of making services online accessible at Service Delivery Centres because these centres are not one-stop centre for service application – for few of the pre-requisite documentation required for service application citizens are required to visit Government offices.

  Sometimes citizens are asked to furnish original copies of documents (submitted online) in-person at Government offices for verification purposes.

- **Service Fees (Expenditure Incurred)**: Actual cost incurred by citizens for availing public services is much higher than the amount stipulated by government. This is because of miscellaneous factors associated with xerox, scan, notaries, etc. that need to be done at the time of application.

- **Service Fees (Payment Mechanism)** – To avail services, citizen often need to pay some nominal fees to the government. In addition, there are utility bills like electricity, water, land registration etc. for which citizen needs to make payment of fees to the government. While a lot of progress has been made in terms of acceptance of different digital payment modes by various government departments, there are still a lot of services who do not provide such ease to the citizens. For many services such as the urban local body services, fees need to be deposited over the counter in the urban zonal offices. After deposit of fees, a challan is provided to the citizen. The citizen then needs to submit a copy of this challan along with other supporting documents at the LSK/CSC to apply for the service through e-District. The entire process is therefore riddled with inconvenience to citizen and involves wastage of time and money.

- **Lack/Absence of updates/information about the status of application**: The applicant is often unaware about application status, reason of rejection, and moreover he/she is often unaware about concerned authority to get required clarity on subsequent steps to be taken for rectification of application. The lack of this transparency causes the citizens to make multiple trips to concerned offices and do unnecessary follow-up with field officials which eventually results in multiple visits, loss of productive time and loss of wage for the citizen.

- **Middlemen**: The citizens often are forced to resort to avail the services of the middlemen to expedite their service application or approval.

b) Problems from Government Perspective

The government also face multiple challenges in terms of service application and approval which are mentioned below:

- **Offline Processes**: The approval process for many public services are still offline which results in considerable delays, leakages, etc. and makes the entire process of service application and approval more cumbersome for Government officers to manage

  Offline process also results in Government offices not having digitized database of the beneficiaries and their data. Though, few Government offices make use of tools like excel/spreadsheets, this does not help ensure reliable data quality. Non-digitized database makes it really difficult and cumbersome for departments to undertake any kind of data analysis and/or create reports for monitoring and review purposes.

- **Notifications**: The approving authority can see the pending applications after logging into the IT systems. The notifications or messages about the pending application in a few IT systems still do not get delivered to them on readily accessible means such as message or email.

- **Service Fees (Payment Collection Mechanism)** – To avail services, citizen often need to pay some nominal fees to the government. In addition, there are utility bills like electricity, water, land registration etc. for which citizen needs to make payment of fees to the government. In electronic payment mechanism, the fee collected online is deposited by the bank in concerned government account in a timebound manner (usually T + 1 basis) with efficient reconciliation mechanisms. While a lot of progress has been made in terms of acceptance of different digital payment modes by various government departments, there are still a lot of services who do not provide digital payment option. For many services such as the urban local body services, fees need to be deposited over the counter in the urban zonal offices or in some cases there may be cash payment option at the government offices. The concerned official will be required to submit the collected cash in the designated government bank account or government treasury. There might be inconvenience, delay or errors in cash management, deposit and reconciliation putting an additional burden on the government manpower.

- **Authenticity of supporting documents**: For approval of applications received online, the approving authority relies on scanned copy of supporting documents and has no means of electronic verification of such documents. Establishing authenticity of scanned copy of supporting documents becomes difficult for Government officers as it may be very difficult to ascertain that the submitted scanned document is a forge document.

- **Authenticity of information:** For approval of applications, the approving authority doesn't have robust measures to validate the identity of applicant as well as submitted information. For example, when the applicant applies for scholarship delivered by Tribal Development Department, the applicant's identity is not verifiable, and the situation becomes more difficult in case of verifiability of private institutions esp. those opened recently. In this case the district

tribal officials need to physically visit the college to assess the validity of institution and the candidate.

- **Inability to detect bogus/ghost and duplicate beneficiaries**: The inability of the government to weed-out bogus or duplicate applications is a major challenge in the approval process. This problem remains as there are challenges with seeding and authentication of Aadhaar (unique identifier) in department database. Removal of bogus/ghost/duplicate beneficiaries can be enabled only through seeding and authentication of Aadhaar across department database.

- **Lack of adequate IT infrastructure**: The online systems require the field officials to grant approval on the IT systems. However, many approving authorities have field duties and are not able to provide adequate time for granting approval through laptop or desktop in their offices. In such scenario, the unavailability of mobility devices (like mobile or tablet device) and inaccessibility of IT applications on mobile devices limit the number of applications processed and consequently causes delays in approvals.

- **Unstandardized and inefficient processes:** The process may be subject to local practices, experience of officials, and there may be unstandardized processes operational across the entire state. In many cases, the information or document being requested from the citizen during application process may not even be necessary.

- **Lack of IT systems and processes to enforce legal provisions:** While Chhattisgarh government has enacted the Lok Sewa Guarantee Act, enforcing the stipulated timelines for service delivery as per the Act becomes a challenge. The challenge arises from the fact that, not all services enlisted under the Act have digital application and approval process. Additionally, even the systems that are online have considerable scope of improvement with respect to both process and technology.

c) Envisioned state

The state intends to transform the process of applying for public service from a citizen perspective. The aim is to move towards a delivery mode where citizen can apply for a service through multiple channels which could include anything from a telephone call or a mobile app or an in-person visit to service delivery centre or a Government office, door-step service delivery (all possible access channels). This would entail making available all G2C service online across multiple channels.

Irrespective of which mode is selected, state wants to ensure that the citizen need not interact or pursue government authorities in any way to get their desired service. Therefore, it will be ensured that there are no repeated visits to government offices or service delivery centres. All citizens will receive periodic updates on the status of their applications via message and emails. In case of rejections or returns, the reason would be explicitly mentioned, and corrective measures explained via email and message. Also, there should be no need to carry and submit supporting certificates/ documents issued by government multiple times. Once submitted, it is to be reused by multiple departments for providing different services.

From a government perspective, state intends to provide online workflow tool to all state departments which can be used by all services to bring their end-to-end approval process online at a rapid pace. For ease and reliability of validation prior to approval, system to system checks between trusted government sources will be enabled. This will ensure authenticity of the applicant identity, supporting documents and affiliations to institutions as applicable. As the system evolves and more data pertaining to citizen and public services accumulate, many routine approvals would be system driven with minimum intervention from the government authorities, thus drastically reducing the workload as well as service delivery time.

The envisioned state for 'Application and Approval' stage of Government to Citizen service delivery can be summarized as:

Increased Access and Awareness of G2C Services	▪ All public services in the state to be delivered online across multiple access channels (mobile app, web portal, service delivery centres (LSKs, CSCs, CHOiCE), Govt. offices, call centre) ▪ Increased penetration of service delivery centres (LSKs, CSCs, CHOiCE) in the state ▪ Information about all public services to be made available to citizens across multiple channels or access points
Submission of data/document only once by citizen and minimal interface with Government	▪ All public services delivery to ensure that there is bare minimum to no in-person visits required for citizen to apply ▪ Citizens to be asked to provide data/document only once ▪ All public services to auto-fetch citizen data/ documents already present with the Government, reducing the obligation with citizen to provide data or submit paper based scanned copies multiple times
Efficient mechanism to validate applicant identity	▪ Applicant/Beneficiary identity authentication done through Aadhaar Authentication service
One stop service fee collection mechanism with provisions for payment through multiple digital payment modes	▪ All public services requiring inward payments from the citizen to government to be integrated with an interoperable payment and settlement mechanism which can lead to seamless delivery of ultimate benefit like a certificate, license etc. ▪ A wide variety of different digital payment options to be made available ▪ All payments (application fee, service delivery fee, etc.) to be enabled at one place
Simplified application forms and standardized requirements of supporting documents	▪ Simplified application forms with departments asking only the necessary data (would require departments to undertake BPR) ▪ Standardized requirements of supporting documents – same set of documents required across the state

System assisted and standardized review and approval process; and access to IT application (for review and approval) on mobile	▪ Most authentication of data/documents and approvals of applications to move from manual towards system-based authentication and approvals, and thus reducing human intervention ▪ Standardized review and approval process across the state
Periodic updates on status of application	▪ Citizens to be periodically informed about the approval status and in case of return or rejection, there should be clear communication of reason and details of concerned authority
Pro-active delivery of G2C services	▪ Basis consent, citizens would be provided pro-active delivery of services (service delivery without the need of citizen applying – as & when citizen becomes eligible)
Effective enforcement of provisions of LSGA	▪ All service under LSGA to be offered online ▪ Effective monitoring of timelines for delivery of LSGA services against the timelines defined in the act ▪ Enforcement of provisions related to timely delivery and penalty on account of delay in delivery of services
Acceptance of digital payment modes on application	All departments will be provided requisite mechanisms to ensure timely, hassle free payment acceptance and settlement. It would be ensured that all modes of digital payments are accepted across all public services contingent upon citizen payment to government. Settlement of these payments received in treasury or respective government bank accounts will be as per industry standards or directives of Reserve Bank of India.

1.3.3. Disbursal of Benefits

The previous section explained about public service application and approval. After approval has been provided, the benefit as per service guidelines needs to be disbursed to the citizen. These benefits can be categorized as (i) **cash benefits** like scholarship and pension and (ii) **in-kind benefits** like food grains, solar pumps; and (iii) Document such as certificate, license, permit, receipt (confirmation of payment, enrolment) etc.

As per DBT norms of the Government of India, the cash benefits should be disturbed by department from its bank account which might be a treasury account or with a commercial bank directly into the bank account of the citizen. Similarly, the delivery of in-kind benefits should be done after requisite authentication of the beneficiary. Both types of disbursal necessitate an MIS which is commonly referred to as the beneficiary management system.

At present, departments are at different levels of IT readiness in terms of having a beneficiary management system with many of them relying on manual processes. Also, disbursal methods vary from one department to the other. Most departments undertake account based NEFT

transfers to the bank account of beneficiaries and do not utilize the central government's platform of Public Financial Management System (PFMS)[1]. All central sector and centrally sponsored schemes are mandated to use the PFMS for direct benefit transfer. While many departments delivering DBT public services are mapped on the PFMS system, only a few services utilize the same for channelizing their payments to beneficiaries.

a) Problems from Citizen Perspective

The citizens face multiple challenges in terms of benefit disbursement which are mentioned below:

- **Lack/Absence of updates/information about the status of benefit/service delivery:** For receiving their approved benefits/service output, the citizen needs to follow up multiple times with the government officers/banks to receive information about their benefit disbursal. In some cases when there is a failure in disbursement, citizens are sometimes not informed about the reason of failure and corrective measure to be undertaken. For non-DBT services, there is lack of information/status about the status of application and output.

- **Delay/Challenge in receiving payments due to unstandardized Payments**: The payments are often done in a decentralized manner at the discretion of the government employees and banks of different districts. This creates unstandardized mechanism of payment timing, frequency or amount across the state. Citizens face challenge of delayed payment and no payment. They also sometimes do not get to know which month's (period) benefit has been transferred to their account. In addition, there are challenges related to payment reconciliation due to which re-initiation of failed transactions gets delayed.

- **Lack of awareness about which bank account is the benefit getting transferred to (Bank Account Mapping Issue):** For receiving their cash benefits, the citizen needs to either provide Aadhaar number (seeded with bank account) or provide bank account number. In cases multiple bank accounts are seeded with Aadhaar, the citizen remains unaware about the bank account to which cash benefit is being transferred. In some cases, the concerned government department force the citizen to open new bank account as per the scheme, this leads to additional confusion in the minds of the citizen. Also, while some schemes would make Aadhaar based payments i.e. benefit gets credited to the account linked to Aadhaar in NPCI Mapper, other schemes make account based payment i.e. the account number provided by the citizen at the time of application (this may also be the new bank account that citizen was required to open at the time of enrolment into the scheme). This aggravates the challenge of lack of awareness about which bank account is the benefit getting transferred to.

b) Problems from Government Perspective

[1] PFMS is an IT system which maps all the source and destination bank accounts involved in benefit transfer. It helps in verification of beneficiary details, just in time fund flow preventing parking of funds, disbursal of payments through both Aadhaar & Bank account enabled modes and obtain utilization certificates for government departments.

The government also face multiple challenges in terms of benefit disbursement which are mentioned below:

- **Leakages due to delivery of benefits to ghost/duplicate beneficiaries**: In most of the schemes, the benefits are disbursed to the beneficiary in their bank account, details of which are not verified. This leads to money being disbursed to unverified account which may belong to individuals who are not beneficiaries of the scheme. Disbursements under many schemes happen from the district level. There are cases where one beneficiary may place multiple applications through multiple districts and in absence of a verified unique identity to de-duplicate them, there is duplication in benefit disbursal. The government does not utilize financial address verification services available in payment platforms such as Public Finance Management System (PFMS). Consequently, only in some services the government can verify the authenticity of the financial address and unique id of the beneficiary. As Government of India mandates use of PFMS for centrally sponsored scheme only, this issue is more prevalent in State Sponsored Schemes.

- **Inefficient utilization of government funds:** The respective Drawing and Disbursing Officers withdraw the designated amount from treasury and park the same in their designated bank accounts. Thus, the government does not get accurate visibility of its entire cash balances, actual amount disbursed to beneficiary, loose interest income and is unable to deploy funds efficiently.

- **Delay in obtaining Utilization certificates:** Due to decentralization, payment mechanism, and practices followed by different regions, there is low degree of standardization. This lack of standardization leads to inconsistent reporting, inadequate control on expenditure, inefficient reconciliation and delayed generation of utilization certificates.

- **Inefficient reporting of DBT data in state schemes:** In absence of robust beneficiary management system, reports on DBT transactions are generated manually and data entry operators often need to enter data into multiple systems. The manual nature and redundancy of data entry activities leads to delay and erroneous reporting of DBT data.

c) Envisioned state

Beneficiary management system and Aadhaar authentication ecosystem required for in-kind benefit disbursement will be provided to all services in the state on basis of requirement provided by respective departments. For cash disbursement, all public services would be linked to PFMS. This will enable verification of bank accounts and propel Aadhaar based payments in the state. Also, there would be provisions for citizen to know which account has been credited with the benefit.

From a government perspective, they would gain more financial control and will have complete visibility on funds present in different government accounts, which will help prevent parking of funds and facilitate just-in-time fund disbursals. Utilization certificates would be generated automatically once all departments start using PFMS for payments to beneficiaries. Leakages

occurring due to duplicate or ghost beneficiaries would be eradicated owing to the Aadhaar authentication ecosystem and beneficiary management systems explained earlier.

The envisioned state for 'Benefit disbursal' stage of Government to Citizen service delivery can be summarized as:

- Timely disbursal of benefits to the correct beneficiaries
- Easy to use provision for citizens to know scheme-wise which account has been credited with the benefit and in which bank account will Aadhaar based payments get credited (which bank account is mapped to Aadhaar in NPCI's mapper)
- Periodic updates on status of benefit disbursal (amount, date, bank account) to be provided to citizens
- All public services dealing with in-kind benefit disbursal to have robust beneficiary management system and Aadhaar authentication mechanism
- All public services dealing with cash disbursement to have robust beneficiary management system linked with PFMS for fund flow and disbursement of benefits to beneficiaries
- Beneficiary Management Systems of state and centrally sponsored schemes integrated with State DBT portal resulting in efficient and auto-update of DBT data on the portal

1.3.4. Feedback and Grievance Redressal

The previous section explained about public service disbursement. Once disbursement is completed, there are limited avenues through which feedback can be obtained from the citizen on various parameters of public service delivery. Presently, e-District services use the Rapid Assessment System (RAS) to get citizen feedback. This system leverages SMS to get feedback from citizens. However, most services in the state do not have a standardized method of obtaining citizen feedback.

Similarly, public grievances can arise across different stages of service delivery lifecycle. However, at present there is no standardized IT enabled platform that can track and resolve grievances. Most citizens approach the grass root or frontline officials with their grievances and there is no stipulated timeline by which it has to be resolved. The quality of response also varies on a case to case basis.

a) Problems from Citizen Perspective

The citizen face multiple challenges in terms of feedback and grievance which are mentioned below

- **Limited mechanism to give feedback**: At present, there are limited mechanisms in the government to provide objective feedback of public services, which can be analysed by government to bring improvements in future. Rapid Assessment System (RAS) is a Government of India system which asks for feedback from the citizens through SMS. However, they have a common template, and usually people do not provide the right phone numbers and/or do not reply to SMS.

- **Cumbersome grievance procedure**: At present, there is no unified and easy to use mechanism to register the grievance. In absence of an easy to use mechanism, the citizens often resort to informal grievance or submit their grievance manually. Given the low rate of literacy in state, the citizen face challenge in submitting written application. For submission of the written application, the citizens are often required to visit District or State Headquarters leading to loss of time and wages.

- **Lack/Absence of transparency regarding updates/information about the status of grievance redressal** : Even when the grievance is registered, there are no updated provided to citizens on the action taken by the government to timely resolve the grievance. In some cases, the grievance may be marked as resolved without solving it to the citizen's satisfaction.

b) Problems from Government Perspective

The government also face multiple challenges in terms of feedback and grievance which are mentioned below:

- **Limited mechanism to collect feedback for improvements:** In most public service delivery, either there is no provision to collect citizen feedback or the feedback is not collected in a structured manner. Due to lack of analysable feedback, the ability of the government to bring improvements gets severely constrained.

- **Lack of mechanisms to track and resolve grievances:** There are a few grievance redressal systems (Lok Swaraj, District Helpline, etc.) which exists in silos and do not address all the services. There are no comprehensive digital systems which can accept grievances, assign them to the concerned individual and track the resolution of grievances as per stipulated SLAs. As a result of this, government fails to address concerns of citizens in a time bound manner which sometimes result in dissatisfaction or mistrust in the government.

c) Envisioned state

It is envisioned that the state will develop a system which can be used by all departments to obtain feedback from citizen. There will be provisions to create customized feedback for each service and obtain through multiple channels viz. a call, SMS, Web form, push notifications on mobile phone etc.

Similarly, there will be a common IT enabled grievance platform which can be availed by all departments. Grievances can be lodged by citizen through multiple channels viz. a call, SMS, Web form, push notifications on mobile phone etc. The department and citizen will be able to track progress on resolution. Accountability and timelines for grievance resolution would be fixed resulting in faster and reliable grievance resolution.

The envisioned state for 'Feedback and Grievance Redressal' stage of Government to Citizen service delivery can be summarized as:

Effective feedback collection from citizens for all public services and analysis of the same to improve delivery of public services in the state	**Making use of an online, multi-channel, customizable mechanism being used by different departments**
Effective redressal of grievances through one stop grievance redressal mechanism for all public services in the state	Making use of a robust digital grievance redressal mechanism, accessible across multiple channels, being used by different departments for registering grievances for all public services in the state, assigning concerned officials for redressal, tracking redressal status and reporting the same to citizens

1.4. Benefits of Envisioned State of Service Delivery to different stakeholders

The tangible benefits of the implementation of the Integrated Proactive e-Governance as potential savings in Direct Benefit Transfer. The World Bank's document states the following:

> *The Government of India DBT Bharat Portal states that Total Funds Transfer in Centrally Sponsored Schemes (CSS) for both Cash and In-Kind Transfers is INR 1,70,377.11 crore in FY 19-20 (cumulative) as per DBT Bharat portal.* ***Estimated savings across all states for these CSS schemes are estimated at 17 percent of expenditure arising from the elimination of duplicate, non-existent and ineligible beneficiaries.*** *The savings accruing to the selected Program schemes are assumed to be of the same order as reported savings on Central Schemes because states implement all schemes and savings from Central schemes comes from state implementation. No explicit savings will accrue in the first three years i.e. 17-18,18-19 and 19-20. Instead we assumed that savings will start accruing from 2021-22 onwards. Total approximate normative budget allocation for selected schemes in 2021-22 and 2022-23 will be INR 13,086,466,159. Applying the national estimated savings rate of 17 percent to the selected state schemes implies that in financial year 2021-22 and 2022-23, the Government of Chhattisgarh will save approximately INR 2,224,699,247. If we average the savings over the project lifecycle, Result Area 4 is expected to yield approximately INR 44.49 crore per year. Therefore, total savings for the last two years of project is expected to be INR 88.98 crore, as compared with total project expenditure for Result Area 4 of INR 70 crore.*

The envisioned stage of service delivery covered in the previous section will benefit citizens and residents, government, and the private sector. Some of the key tangible benefits to the stakeholders are described below:

1.4.1.1. Citizens and Residents

- Citizens will get hassle free, assured and on-time delivery of government services and benefits.
- Citizens will get easy and direct access to the government without any intermediaries

- Increased convenience
  - All public services online and at service delivery centres across the state
  - Doorstep service delivery
  - Documents/Data to be provided only once
  - Proactive and 1-minute service delivery
  - Single interface to interact with Government (One app, One portal, One login)
- On time delivery of benefit amount directly into bank accounts
- Unified Grievance Redressal – One place for all grievances
- Data driven design of schemes
  - Targeting right beneficiaries
  - Minimizing exclusion/inclusion errors
- High transparency – Enhanced visibility into the processing and delivery of services

1.4.1.2. Government

Leadership	• The political leadership will be able to win the trust of the people by making public services accessible, transparent and convenient • Reduction in inefficiencies in public service delivery will allow more fiscal elbow room to plan and launch new schemes for socio-economic development of the state • Accurate targeting of the beneficiaries • Data driven governance will allow the government leadership to have better situational awareness of the welfare initiatives while they are being rolled out on the ground. • Better monitoring of welfare initiatives
Policy Makers	The policymakers will have access to the right tools and accurate data and insights to design effective policies for the state
Administrators	• Zero cost to enable online service delivery for departments - Make available all G2C services online (Accessible across Service Delivery Centres across the state, Mobile App, Web portal, Call Centres) • On-time transfer of monetary benefits into citizens' banks accounts (DBT through PFMS for all state schemes) • Access to real-time performance data to take targeted actions • High transparency
Field Staff	The digital tools will enable the government staff providing the services at the last mile to do so with higher confidence, more effectively and will reduce the probability of errors.

1.5. Key Stakeholders

IPeG is a transformational program which will involve a wide variety of stakeholders. The stakeholders have been category as Internal Stakeholders which are internal to the Government of Chhattisgarh and External Stakeholders which are outside the Government of Chhattisgarh. The key stakeholders have been listed out in the table below:

Stakeholder	Benefits or Role/Participation
Internal Stakeholders	
DIF - Directorate of Institutional Finance, Finance Department, GoCG	Nodal body for implementation of World Bank's Chhattisgarh Public Financial Management & Accountability (CPFMAP[2]) Program
CHiPS	The implementing agency for IPeG project under CPFMAP program. The enabling agency who will be responsible for: • Design, implementing and maintaining the IPeG solution, • Design and implement all the technology solution components envisaged under IPeG • Establish/utilize the shared infrastructure which can be utilized by all departments • Handholding the line departments for bringing transformation in their service delivery including technical and functional support services to line departments • Undertake Change Management and Capacity Building Exercise

[2] World Bank Program Appraisal Document (http://documents1.worldbank.org/curated/en/858051551063626207/pdf/India-Chhattisgarh-Public-Financial-Management-and-Accountability-Program-Project.pdf)

Stakeholder	Benefits or Role/Participation
Line Departments that deliver G2C services, welfare benefits through DBT	All these departments will have one, some or all the following benefits: • End to end digitization of service delivery workflow • Better beneficiary data quality • Robust beneficiary management system • Reduced turnaround time, cost and effort for delivery of service • Reduced leakages and pilferages in service delivery • Better tracking and resolving of public grievances • Better policy planning through availability of wide range of anonymized, secure beneficiary data Some departments like the Food and Civil Supplies Department may also play a role of enabler. Using the Public Distribution System (PDS), the social beneficiary database under the IPeG program may be initiated. All the departments will also have to comply with provisions of applicable laws/regulations around Aadhaar, Data Privacy/sharing, Data Exchange Policy drafted for exchange of data under IPeG program, Lok Sewa Guarantee Act (LSGA), relevant provisions of IT Act and other applicable laws/regulations.
District Administration	Implementation of processes and systems at the field level to enable service delivery
External Stakeholders	
Residents of Chhattisgarh	• Enhanced quality and ease in availing core and enabling services at the initial stages • Reduced time, cost and effort to avail all G2C services • Pro-active delivery of services, without them having to apply for it
Government of India	Provide the policy frameworks and standards for e-Governance, Digital Services, Digital Payments, etc.

Stakeholder	Benefits or Role/Participation
The World Bank and its Independent Verification Agent	They are responsible for providing loan to carry out the execution of IPeG project as a part of Chhattisgarh Public Financial Management & Accountability Program. There are Disbursement Linked Indicators (DLIs) which the state government needs to achieve and upon achieving it, World Bank will release funds post verification of DLIs. The verification of the DLI will be performed by the Independent Verification Agent (IVA) which has been selected by the GoCG. This IVA will evaluate the attainment of disbursement linked indicators (DLIs) finalized with the help of the World Bank. Only, after the DLIs have been met as per conditions set, will the World Bank release the requisite funds.
Service Delivery Outlets and Doorstep Delivery Agents	Provide support to the residents in availing the public services in assisted mode of service delivery
Private Sector Entities	Utilize the data and service for the purpose of delivering their services to end-customers
Non-Government entities, Research agencies and Academia	Utilize the open data for purpose of research and innovation
Consultancy Firm	Provide design and implementation support and subject matter expertise for design and implementation of the planned initiatives
System Integrator (s) (to be selected)	Design, Development, Operations and Maintenance of IT solutions under IPeG project

2. SOLUTION OVERVIEW

Different interventions across process, technology and legal frameworks would need to be carried out to achieve the objectives of the program. The technology interventions would specifically need assistance from the incoming System Integrator. In following sections, design principles have been outlined for understanding of bidders and an overview has been provided on the technology interventions that would be required under the IPeG project. The exact scope of work is a subset of these interventions and have been outlined in the upcoming sections.

2.1. Design Principles

The principles of the design are fundamental rules which must be adhered to, during the design and implementation of the program. They act as a guide in decisions involving complex and ambiguous scenarios. The following design principles have been envisaged for the IPeG program:

- **Autonomy and Choice:** The departments should have the autonomy to design and operate their public services and they will also own the corresponding data. They should also have the choice to use some or all services from bouquet of services offered by IPeG platform. Similarly, the citizens should also get multiple choices to access and avail the public services.
- **Evolving by Nature:** The departments should be able to go through its service delivery maturity curve as per its own context. The services offered to the departments as well as the citizens should also evolve with time and requirements.
- **Citizen Centric:** The main outcome of the program is to increase citizen's convenience. Thus, the entire experience of the citizen in public service delivery should be designed so as to provide maximum convenience to the citizen.
- **Inclusive:** The program benefits should reach all sections of society without any barriers irrespective of their social, economic, physical, and educational status.
- **Minimalistic:** Only those components, services will be developed and only those data elements should be captured and stored which are bare minimum to achieve the intended outcomes. Also, the program should be designed in a manner that requires minimum efforts and cost.
- **Reusable and Shared Assets:** The program should be designed in a manner to reutilize and share the assets i.e. components, services, data, processes, people, facilities, infrastructure, etc.
- **Management by Exception**: In the normal course, decisions should be based on pre-configured rules and procedures with minimal human discretion. Administrative interventions should be needed only in exceptional cases, the causes of which should be addressed to reduce the number of such instances.

- **Privacy by design:** The principles of privacy should be embedded in the design and there should minimal or no discretion or authority to overrule the privacy provisions.
- **Democratisation:** The program should democratise creation and consumption of assets (processes, data, services, tools, etc.). Authorized government and private entities should be able to repurpose, extend, customize, and contextualise some of the assets to suit their own needs and context. Non-personal, non-sensitive and aggregated data should be emitted to be used by wider stakeholders.
- **Modular**: Each component should be minimalistic, independently replaceable and extensible. The interaction amongst various components should be managed through standards-based protocols (plug-and-play).
- **Scalable:** The program is intended to deliver the public services to all citizens and departments. The components and utility of the program is expected to start small but grow to scale, thus all the components should have the provision to extend and scale.

2.2. Technology Interventions

2.2.1. Business Requirements

The broad business requirements that technology interventions under IPeG need to cater to, basis the envisioned state of service delivery across the lifecycle of service defined in the previous chapter, are described below:

- **Service Discovery, Application, Approval and Delivery**: This comprises end-to-end process of public service delivery i.e. service discovery, service eligibility check, authenticate identity (identify applicant), submission of application for services, fetch data from connected trusted data sources through data exchange platform, payment of service fee by citizens, tracking of application status, validation/scrutiny/review/approval of submitted application, disbursal of service output (certificate/intimation/monetary benefits/in-kind benefits)to the citizens, etc.
- **Grievance Redressal:** This comprise of set of services relating to end-to-end process of grievance management i.e. grievance submission, tracking of grievance redressal status, management/monitoring of grievance, resolution of grievance and reopening of grievance.
- **Scheme Analysis and Policy Planning**: This comprise of set of services relating to end-to-end process of scheme analysis and policy planning i.e. analysis of existing schemes, data ingestion/upload, data analysis and visualization, budgeting and design of new schemes/policies, etc.

These broad business requirements would be catered to by a number of service and solution components that would be offered by IPeG.

2.2.2. Functional Architecture

The IPeG solution comprises of the multiple layers which are as follows:

- **Business Services**: These are broad business services that IPeG plans to deliver to the end users (Citizens/Government users) as part of the business solution covered in previous section. To enable delivery of these broad business services, a number of technology solution components would be required.
- **Users**: The IPeG would be accessible for different types of users which will utilize it to deliver the above business services.
- **Access Channels**: The IPeG would be accessible over multiple channels (web, mobile, service delivery centres, Govt. offices etc.). This will ensure that the services provided by IPeG are available to users in a manner which is convenient to them.
- **IPeG Toolkit:** This will be a set of components which can be utilized by the onboarded departments to (i) deliver their services without needing to establish their own IT systems, and (ii) augment their services by plugging the toolkit(s) into their existing IT systems.
- **IPeG Platform:** Th**e platform** will be responsible to deliver a set of services to different Government departments/organizations. The platform will have components such as Platform Services, Data Exchange Platform, Data Sources etc.
- **IPeG Internal Systems**: For entire solution to work efficiently, the internal systems will be utilized.
- **Infrastructure and Operations**: The infrastructure will be established, and operations will be performed from the perspective of hosting infrastructure, network, software and security.
- **External Systems**: IPeG system will interact with external systems, from Government of India and Government of Chhattisgarh, to deliver the services under IPeG.

The diagram intends to provide a holistic view of all components in IPeG that have been discussed and represents the functional architecture under IPeG.

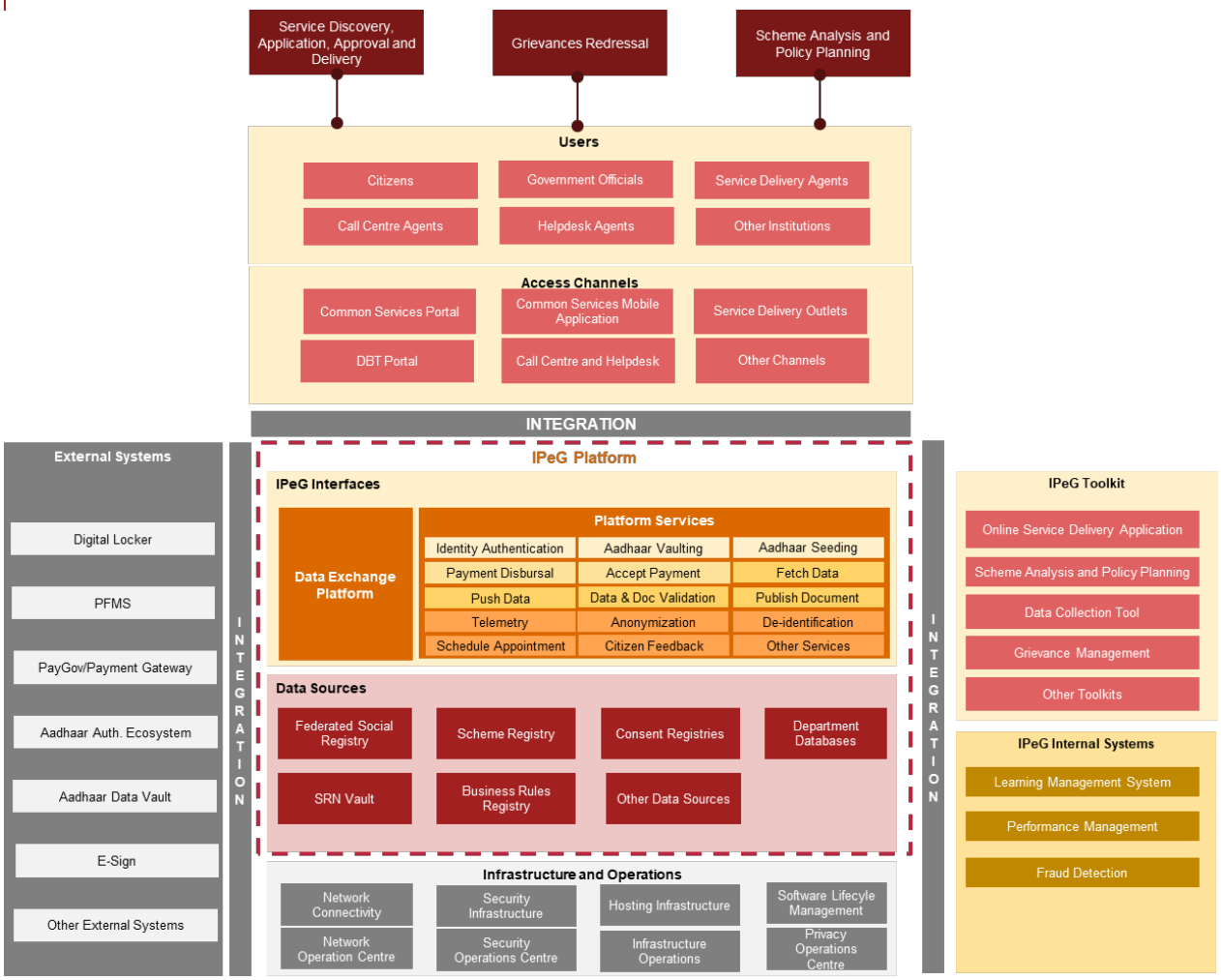


Figure 2: Functional Architecture

2.2.3. Technology Solution Components

The different technology components can be broadly be classified as:

1. **Toolkit** - These will be set of applications/tools which can be utilized by departments to cater to their requirements. Departments may choose to use all applications/tools/services offered as Toolkit or they can choose to use only a select few applications/tools/services. The purpose of these tools would be to minimize investments to be made by different government entities in developing/purchasing the same application for the same business need.
   Some of the departments may already be using some IT application which is similar to the ones offered under IPeG toolkit. These departments may either continue to use their existing systems or migrate to applications/tools offered as IPeG toolkit.

2. **Platform Services** - The IPeG platform will offer a set of services which can be used by public service delivery systems used by different departments. The platform-services would be made available to both:
    a. Departments using their own service delivery/other applications (In this case for departments' applications to be able to consumer platform services, they will need to adhere to a set of digital standards to be published by CHiPS for IPeG program)
    b. Departments utilizing the service delivery application/other applications provided as IPeG toolkit solutions.

    These platform-services will function as independent units having defined input and output protocol which will enable it to be developed, maintained, and scaled independent of one another. The departments may choose to use one or more of these services.

3. **Data Sources (Social Registry)** - The data sources are trusted sources of data elements (information and documents) which are required for the purpose of public service delivery to the citizen. One of the key pre-requisites to enable achievement of envisioned state of service delivery is exchange of data between departments. Data sources are trusted sources of data residing in different departments that would store and share data with other data sources/applications.

4. **User Access Channels and associated Technology Components**: These components are front-end interfaces to the end users. The IPeG program is experienced by the end users through these interfaces.

It may be noted that Toolkit solutions offered under IPeG would be designed in a way to enable consumption of Platform services offered under IPeG and interact with Data Sources onboarded onto IPeG platform, and integrated with user access channels and associated technology components, as per requirement. For e.g. Service Delivery Application (BPM) would be integrated with Common Services Portal (Web and Mobile application), DBT Portal (for DBT schemes onboarded onto Service Delivery Application), Single Sign-on.

The brief explanations of different technology components are given below:

Component	Brief Description
1) Toolkit	
Service Delivery Application	This toolkit may be used by the departments to digitize their entire process flow i.e. application form, payment receipt, workflow, and output (certificate and direct benefit transfer).
Grievance Redressal Solution	The IPeG aims to create a unified platform to manage all grievances across the state of Chhattisgarh. This module will be used by citizen to lodge grievances, notify relevant government departments of new grievances, delegation and resolution of grievances, escalations for SLA breaches for existing grievances and generation of reports for monitoring purposes. This system will also be integrated with existing grievance management systems, if any, of the departments.

Component	Brief Description
Scheme Analysis and Policy Planning	This solution will help the departments to analyse information and create actionable insights, reports, dashboards, and insights using the vast amount of data spread across the departments. Based on information available with government across its different department databases, the policy planning tool would help departments to: • Monitor the effectiveness of operational schemes • Enable the design of new programs, schemes and policies • Undertake scheme budgeting and rationalization
Data Collection Tool	This tool shall assist departments to collect data and enhance data quality. It will assist in improving quality of existing database for a department and also enable collection of high quality data through user friendly interface and pre-defined, easily configurable business rules of data validation.
Advanced Analytics Tool	This tool will be used by departments to undertake statistical modelling and rule-based analysis to get detailed insights into how their schemes are being implemented. The analytics tool will allow the user to use statistical models to perform Advanced Analysis, Business Intelligence etc., Departments can fetch cross department data in a de-identified form to run statistical models
2) Platform Services	
Category 1 – Aadhaar Related Services	
Aadhaar Vaulting	The government entities will be able to use the services of the Aadhaar Data Vault for securely storing the Aadhaar number collected by them for delivery of respective services. Departments in return will get a Reference Key, unique for an Aadhaar number, generated by the Aadhaar Data Vault system, that they can store in their systems. 'Aadhaar Vaulting' as a service would prevent all departments to set up their own separate Aadhaar Data Vaults resulting in significant cost and effort savings. Centralized Aadhaar Data Vault maintained by CHiPS under IPeG, would cater to Aadhaar Vaulting needs of all the government organizations in the state.
	Enabling System

Component	Brief Description
	Aadhaar Data Vault will be provided by CHiPS, which would act as an enabling system to provide 'Aadhaar Vaulting' service to all Government organizations of Chhattisgarh.
Identity Authentication (Aadhaar Authentication and non-Aadhaar based) and obtain demographic details (e-KYC) as in Aadhaar	For delivering the public services, the government departments may be required to authenticate the citizens and/or obtain their demographic details. IPeG program would help facilitate identity authentication as (a) Aadhaar based identity authentication, and (b) Non-Aadhaar based identity authentication. **Enabling System** Aadhaar Authentication Ecosystem will be provided by CHiPS, which would function as AUA (Aadhaar User Agency) or ASA (Aadhaar Service Agency) and provide departments the service to authenticate identity and fetch demographic data (e-KYC) as in Aadhaar
Aadhaar Seeding Validation	Once Aadhaar is seeded in department database, there might be two levels of validation a department might need to perform. One, whether the Aadhaar number itself is a valid or correct number and two, whether the Aadhaar number is seeded against the right beneficiary information. Additionally, department might have the need to validate whether, the Aadhaar number is linked to a bank account to initiate Aadhaar based payments. The Aadhaar seeding validation service will cater to all these three needs of a department, ensuring accurate Aadhaar seeding in department database. **Enabling Systems** This service shall be provided through a combination of: 1) Front-end validations like application of Verhoeff algorithm to verify sanctity of the Aadhaar number itself 2) Integration with Aadhaar authentication ecosystem to check whether the combination of Aadhaar number and demographic details in beneficiary database of departments match with the combination of Aadhaar number and demographic data as in Aadhaar, and seeding has been done accurately or not. 3) Integration with NPCI mapper to check linkage of Aadhaar number and bank account

Component	Brief Description
Category 2 - Payment related services	
Benefit Disbursal through PFMS/ iFMS	This will be a standard service of 'Benefit disbursal through PFMS/ iFMS' for DBT schemes of departments. This shall enable these DBT schemes to make cash disbursal to its beneficiaries through PFMS system of Government of India/ iFMS system of GoCG. **Enabling System** This service would be enabled through a 'Platform for payment through PFMS/ iFMS' , which would act like a bridge between different scheme systems and the PFMS/ iFMS system.
Accept Payment (from applicant) Service	The government is expected to accept payment of fees to provide public service and citizen is expected to make a payment of fees to government for availing public services. To increase the convenience of citizen, the government should enable the multiple modes of payment such as UPI, IMPS, Internet Banking, Debit Card, Credit Card, etc Applicants should be provided the facility to make different payments (service fee, service charge etc.) through multiple digital payment modes at the time of submission of application. **Enabling Systems** • Integration of service delivery application with different digital modes of payments • Settlement and reconciliation system to settle payment collected from applicant among different agencies involved in service delivery
Category 3 – Data related services	
Fetch Data/Document	When the citizens requests for service delivery, this service will be used to fetch data/document from registries as well as other public service database and auto-populate the service application forms using the fetched data. This service will also be used at the time of verification of these application forms by the government officials. **Enabling System**

Component	Brief Description
	Data Exchange Platform and associated data sources - A data exchange platform would be developed that shall enable exchange of data/documents between different departments/government organizations of Government of Chhattisgarh. This platform shall be governed by a Data Exchange Framework and Guidelines. Fetching of data from different data sources (Federated Social Registries, other registries, databases) would be facilitated through Data Exchange Platform.
Push Data/Document	When the citizens' data gets updated in the trusted source, this service will be used to inform other databases/registries, which have subscribed to such updates/changes. **Enabling System** Data Exchange Platform and associated data sources
Data and/or Document Validation	This service can be used to match the available data/document against the data/document stored in registries and public service databases. One of the use case is when the government official wishes to validate the data/document submitted by an applicant to avail a public service - this platform service will be used to match the data/document received during the application submission and will be verified against the data/document present in the concerned trusted data source. . **Enabling System** Data Exchange Platform and associated data sources
Publish/Fetch documents to/from Digi locker	The departments or the citizen themselves can store/fetch issued documents (e.g. marksheets, certificates) to/from the Digi-locker. This service may be used by the departments to publish/fetch their documents to/from the digital locker with due consent from the citizen. **Enabling System** Data Exchange Platform and Digi-locker
Anonymisation of data	To ensure the privacy of citizens data, there will be a need to anonymize the citizen's data. Through anonymized data it is not feasible to identify the individual to whom the data corresponds to. This will be useful for use-cases of analysis of schemes and design of new policy/schemes, etc.

Component	Brief Description
	Through this service, departments would be able to anonymize their data. Beneficiary database of departments would be the 'input' and they would receive 'anonymized data' as an 'output'.
De-identification of data	To ensure the privacy of citizens data, there will be a need to de-identify the citizen's data. Through de-identified data it is feasible to re-identify the individual to whom the data corresponds to. This will be useful for use-cases of data analytics, policy planning, etc. Through this service, departments would be able to deidentify their data. Beneficiary database of departments would be the 'input' and they would receive 'deidentified data' as an 'output'.
Telemetry	This service will be used to generate a stream of analysable anonymized input about system behaviour. The stream of data generated through this system, Processes, Integrations can be utilized to improve the system, Process, performance and also designing new schemes.
Category 4 – Other Services	
Collect Feedback	This service will be used to collect citizen feedback and satisfaction. The feedback will be collected for each interaction of the citizen with the government for public service delivery.
Schedule Appointment	This service will be used by the citizen, service delivery agents or government department to schedule appointments on basis of business requirements like doorstep delivery, re-submission of documents based on return remarks provided by approving authority etc.
Messaging	This service will be used to email notifications and message alerts to the citizens and government departments, depending upon business requirement.
Translation	This service will obtain the data in one language and translate the data in another language.
Single Sign-On	This service will be used to do enable the Single Sign-On for citizens and government users across all applications integrated with Single Sign-on **Enabling System** This single sign-on application will be designed to integrate all the different applications for service delivery used by different

Component	Brief Description
	departments under a single authentication domain. It is a centralized session and user authentication service in which one set of login credentials can be used to access multiple applications. The service authenticates you one on one designated platform, enabling the user to use all services without having to login and logout each time. Once the user logins to the SSO, all the services that comply SSO integration will be auto-logged in by sharing SSO session. After login to SSO, the user can move seamlessly between multiple services (services integrated with SSO).
3) Data Sources (Social Registry)	
Federated Social Registry[3] (Centralized and Decentralized)	The registries are trusted sources of data elements (information and documents) of residents' whose native state is Chhattisgarh and people living in Chhattisgarh state) of the state, which are required for the purpose of public service delivery to the citizens. Social registries containing citizen data would broadly be of following two types: • **Federated Social Registry (Centralized):** This would centrally store some commonly used resident data at one place viz. Name, Date of birth, Gender, Address, Ration card number, Aadhaar Vault ID (Reference number) etc. The exact set of data fields will evolve and get finalized during course of the project. • **Federated Social Registries (Decentralized):** These registries would store information about residents specific to particulars schemes/service. This will be hosted by concerned departments which are owners of respective information. A few examples of fields in this registry are disability status, Highest Degree Name and Year, etc. • **SRN Vault** The IPeG model is based on two ID concept, one foundation ID (Aadhaar) & another functional ID named as Social Registry ID Number (SRN ID). For enabling data exchange between departments (those departments integrated with IPeG ecosystem), SRN ID is required to generate and seed in department databases along with

[3] "Registries are shared digital infrastructure onto which authorized issuing agencies publish digitally signed data about users, entities, or other assets/resources allowing consented and controlled access to other authorized service providers for digital verification and usage."

Component	Brief Description
	Aadhaar reference ID against each beneficiary. Using SRN as functional ID, data exchange gateway will facilitate the departments for secure information exchange between Information Users (Citizens, Departments, Call Centre Agents, Service Delivery Agents, etc.) and Information Providers (Federated Social Registries, Other Registries) through a pre-defined data exchange rules and protocols.
Public Services Registry	The government delivers various public services to the citizens. Each of these public services have its unique features i.e. eligibility conditions, application data elements, access points, process, timeline, fees, etc. This registry will store the information about these unique features. This registry will be used to respond to citizens enquiry about these public services as well as during the proactive service delivery to the citizens. Every public service/scheme shall have a unique 'Public Service ID'. This ID shall be used to uniquely identify a Public Service under IPeG program.
Rules Database	This database will contain all the business rules. A key purpose of this registry will be to store codified rules as defined in the Data Exchange Policy which will form the basis for Data Exchange Framework.
Consent Repository	The collection, storage, processing/authentication and exchange of data may require consent from individual to whom the data belongs, depending upon nature of the data being shared and the legal framework governing the same. During citizens' interaction with IPeG program, required consent from citizens as per extant laws/Data Exchange Policy of IPeG program, will be obtained in electronic format as per Electronic Consent Framework' of MeitY. Every department will maintain its own set of consent obtained from citizens. The feature to obtain and store consent would be made available in BPM solutions offered under IPeG. However, if a general consent for use in IPeG program is obtained from a citizen, this will be stored by CHiPS in a 'Consent Repository' under IPeG program.
Other Registries and Index of Registries	Over a period of time, as the program gets rolled out, other registries to meet the requirements of departments and IPeG system, shall be created and rolled out. An index of registries shall also be created, that shall contain:

Component	Brief Description
	i. List of all the registries under IPeG program, and what it stores ii. Data fields - All kinds of data viz. negative list, data fields for whom masters have been defined along with names of such masters, data field for whom master have yet not been defined. iii. Other data fields, as required, as the program gets rolled out
4) Access Channels	
Common Services Portal	In the proposed scenario, all public services would be accessible to citizens through a common portal irrespective of whether the departments use an existing application or application for online delivery of services (BPM solution) offered under IPeG. This 'Common Services Portal' would be accessible to service delivery agents across the state – LSKs, CSCs, CHOiCE Centres, citizens and government users. Departments, which currently offer their services through their own portal would need to offer their service on this Common Services Portal in addition to offering it on their portal, once onboarded on IPeG. They may also choose to discontinue their own front-end portal after having listed their service on the common front-end portal (Common Services Portal).
Mobile Application	This app will provide the same range of functionalities as that of the common services portal on mobile platform. It will act like an aggregator wherein all public services of Chhattisgarh can be availed through this single app for citizens. Similarly, government officials can access this app and perform their monitoring and approval duties as per public services allotted to them. The number of public services made available through this app will keep increasing as more and more public services are onboarded to IPeG.
State DBT Portal	Portal for maintaining DBT data about the various Direct Benefit Transfer (DBT) schemes operational in the state of Chhattisgarh. This portal is in turn integrated with the National DBT portal (DBT Bharat). State DBT portal shall also be integrated with different beneficiary management systems of the state including the service delivery application (BPM) offered under IPeG to facilitate fetching of DBT data onto State DBT portal from these systems.

To enable implementation of the above-mentioned technology components, enabling technology systems that need to be in place or the systems with which the above-mentioned technology components would interact are capture below.

Component	Description
Infrastructure and Operations	
Hosting Infrastructure	The IT and Non-IT systems necessary for hosting the IPeG solution will comprise of virtual environment (cloud) with a business continuity setup. This infrastructure should be able to start with the initial requirements and should be scalable to meet the long-term requirements of the program. To prevent vendor lock-in, this should be built on the commodity infrastructure and should be portable across different MeitY empanelled Cloud Service Providers without any major software code change. The administration, maintenance and operations of the hosting infrastructure for IPeG program will be carried out by the MSI
Software Lifecycle Management	Since IPeG platform applications are proposed to be on Microservice based architecture, it is essential that end to end automation of development, testing and deployment happens through DevSecOps. It is proposed to be scalable platform for automation of CI/ CD/ CT (Continuous Integration/ Continuous Development/ Continuous Testing) activities as a centralized DevSecOps implementation. Each application under IPeG platform would have their own environment for the development cycle, including code configuration management, build, packaging, deployment and system testing. This should happen through container-based platform and once system tested, container would be deployed on staging environment.
Call Centre	To manage all inbound citizen interactions with IPeG there will be a call centre. The call centre will be used for status check of applications, raising grievances related to IPeG onboarded schemes, eligibility check of schemes or obtaining scheme information etc.
Technical Helpdesk	The technical helpdesk will be utilized to lodge and monitor the incidents reported as well as technical alerts generated by the solution.
IPeG Internal System	
Performance Management	This solution will enable monitoring of the performance of people, process and technology systems. The desired

Component	Description
	performance levels will be codified in this solution which shall be compared with observed values for the various identified parameters. The deviations will be reported to the concerned authority for initiation of corrective measures.
Fraud detection	The fraud detection system will be utilized to identify, lodge, assign, monitor and report the potential frauds.
Data Exchange Gateway	Data Exchange Gateway includes both software development/API development standards as well as the set of actual APIs that will enable data exchange between different systems inside and outside IPeG. For configuration, request submission and request approval/rejection management, it will have a configuration interface. All stakeholders will only receive the requested data as a result of data exchange framework being in place but only those responsible for coding or configuration will be able to access it
External System – Integration with IPeG	
Digital Locker	The DigiLocker of the MeitY is a shared infrastructure aimed at the purpose of paperless governance, created for the purpose of providing access to authenticated documents to the citizen's digital document wallet. The issued documents in DigiLocker system are deemed to be at par with original physical documents.
PFMS & IFMIS	There are various social welfare schemes of Central Government and State Government where benefits are required to be transferred to directly into the beneficiaries' bank account. This system will enable the departments to: • Validate the beneficiaries bank account, • Manage disbursal of benefits directly into bank account of beneficiaries, and Improve financial management (through just-in time release of funds, and monitoring of use of funds including ultimate utilization)
PayGov	NSDL Database Management Ltd (NDML) on behalf of MeitY has created a common infrastructure that can be used by Center/States/Departments to offer various services through their national/state portals with a facility to make online payment. PayGov India offers a range of payment options (net-banking, debit card, credit card, IMPS, cash cards/wallets, NEFT/RTGS,

Component	Description
	BHIM/UPI) through which a payment can be made by the citizen to avail a service.
Open Data Portal	OGD is a platform for supporting Open Data initiative of Government of India. The portal will be used to contribute open data by the Government of Chhattisgarh.
E-Taal	e-Taal is a platform for dissemination of e-Transaction statistics of National and State level e-Governance Projects including Mission Mode Projects. It automatically pulls the e-Transaction data from applications integrated with it using Web Service technology and facilitates quick analysis of transaction data for the user.
E-District	E-district is a mission mode project being implemented by CHiPS. It is a platform used for delivering nearly 110 government to citizen services, clocking more than 3 lakh transactions per month with a total of 1.37 crore transactions till date. Citizens can access the services from Citizen kiosks (CSC/Lok Sewa Kendra), Web Portal and Mobile application.
E-Sign	eSign service allows applications to replace manual paper based signatures by integrating an API which allows an Aadhaar holder to electronically sign a form/document anytime, anywhere, and on any device legally in India. eSign service facilitates significant reduction in paper handling costs, improves efficiency, and offers convenience to customers

2.2.4. Technology Architecture

The key building blocks required to develop and operationalize IPeG platform are depicted in below diagram.

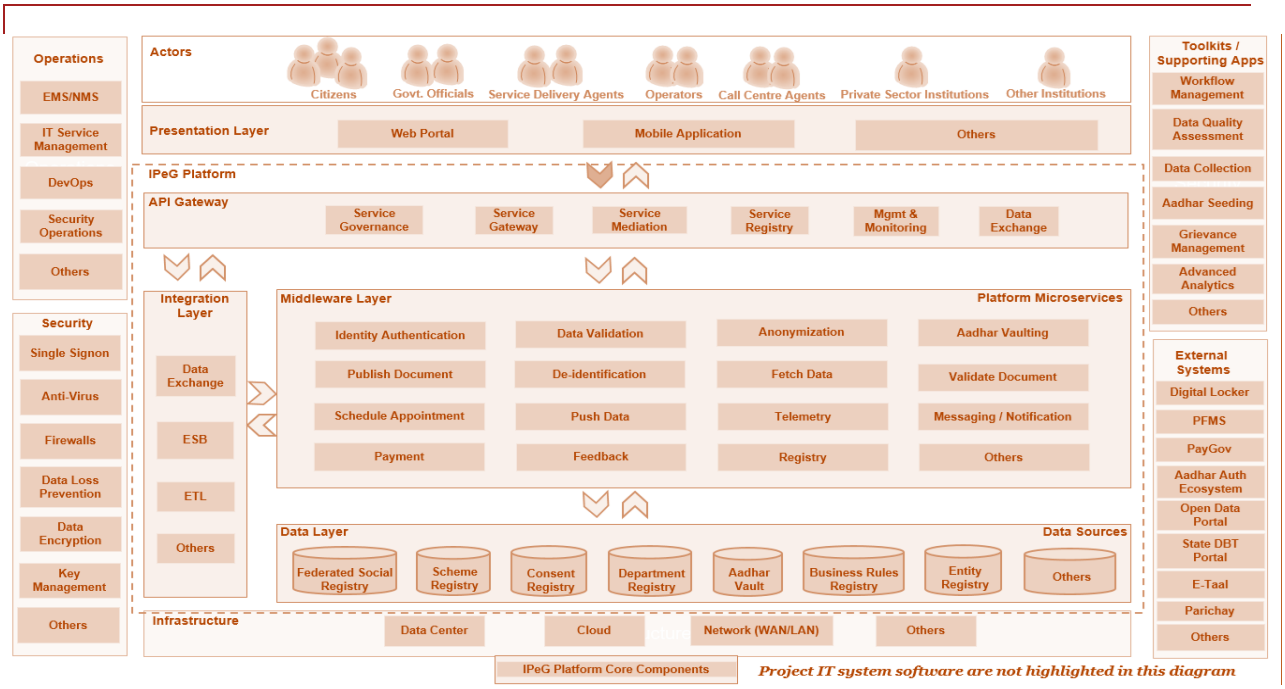


Figure 3: Layered Architecture

The IPeG solution comprises of the multiple layers which are as follows:

- **Actors**: The IPeG would be accessible for different types of users which will utilize it to deliver the above business services.
- **Presentation Layer**: The IPeG would be accessible over multiple channels (web, mobile, etc.). This will ensure that the services provided by IPeG are available to users in a manner which is convenient to them.
- **Middleware Layer**: All application and core services under IPeG platform are envisaged to be developed using microservices. Under microservice architecture, all applications are composed of small business domain centric services. These services can be deployed independently of one another. These services are loosely coupled with each other. The microservices will be focused on completing a dedicated task in an efficient manner. Microservices architecture would be enabled through tools for service discovery, packaging standards for containerizing applications, continuous integration.
- **Integration Layer:** The integration layer will provide integration for internal and external systems. The integration layer will contain different components such as Data Exchange Gateway, Enterprise Serial Bus (ESB) and Extract Transform Load (ETL) applications.
- **Data Layer**: The data sources for the IPeG program will reside in this layer. This will comprise of Federated Social Registry Scheme Registry, Consent Registry, Department Registry, Aadhaar Vault, Business Rules Registry, Entity Registry, etc.
- **Infrastructure Layer**: Infrastructure to host IPeG platform including data centre/cloud environment, network and security.
- **Toolkits**: The Toolkits are the consolidation of all the sample supporting applications & in the IPeG platform that effectively can be used by departments & customized to provide service delivery to citizens and other stakeholders. The toolkit components are outside the IPeG platform.
- **External Systems**: To deliver the services, IPeG will interact with the existing IT systems of the Central Government as well as State Government. The external interface layer will

interact with such external components viz. e-Sign, Digital Locker, PFMS, Aadhaar Ecosystem etc.

- **Operations**: The operations will comprise of Enterprise Management System (EMS), IT Service Management, DevOps, and Security Operations.
- **Security**: The security will comprise of Single Sign-On (SSO), Anti-Virus, Firewalls, Data Loss Prevention (DLP), Data Encryption, Key Management, etc.

3. SCOPE OF WORK

3.1. Overview on Scope of Work

The overall tenure of project is 3 years, with possibility of extension for 2 years on need basis at the discretion of CHiPS. The scope has been divided into three tracks. In 1st year the MSI needs to complete the three tracks listed below. For remaining two-year MSI will continue the O&M along with onboarding any new scheme identified.

- **Track 1: IPeG Solution Implementation [Refer Section 3.2 to 3.13 for details]**
    - Solution Implementation
        - Cloud Infrastructure Provisioning
        - Software Design, Development, Integration, Testing and Security Audit
        - Call Centre and Helpdesk Setup
        - UAT and Go-Live
- **Track 2: Mandatory onboarding of 5 select schemes on IPeG solution (Deliverable Basis) [Refer Section 3.14 for details]**
    - Scheme Study, Digitization and/or Integration of IPeG Solution Components
    - Cleansing of existing data and/or configuration of IPeG components for data collection
    - Technical support (API development, etc.), training and handholding of end-users
- **Track 3: Demand driven onboarding of 45 schemes and data sources on IPeG Solution (Time and Material Basis) [Refer Section 3.14 for details]**
    - Scheme Study and Government Process Reengineering
    - Digitization and/or Integration of IPeG Solution Components
    - Cleansing of existing data and/or configuration of IPeG components for data collection
    - Technical support (API development, etc.), training and handholding of end-users
- **O&M [Refer Section 3.5 & 3.13 for details]**
    - Operations and Maintenance (O&M will start component wise on successful UAT and will continue for the entire contract duration)
        - Cloud Operations and Maintenance
        - Software Operations and Maintenance

- Call Centre and Helpdesk Operations

The key list of activities that need to be undertaken by the MSI are provided below.

- **Project Planning and Solution Design:** The MSI needs to finetune the detailed project plan in consultation with CHiPS. MSI will be responsible to gather the detailed requirement for IPeG solution components, revise the FRS, finalize the design and requirements. The design should cover various usage scenarios, volume estimation, integration scenarios, etc.

- **Software Customization and Configuration for Toolkits**: The MSI will be responsible to provide COTS/OTS product(s) and configure/ customize them as per finalized requirements. The exact set of requirements will be firmed up further during the requirement gathering and design stage.

- **Software Development and Implementation Platform Service, Data Sources and Access channels**: The MSI will be responsible to develop, test, integrate, and implement the platform service, data sources and access channels as per finalized requirements. The exact set of requirements will be firmed up further during the requirement gathering and design stage.

- **Installation and Commissioning of IPeG solution components:** MSI is responsible for provisioning of cloud infrastructure on Virtual Private Cloud (VPC), preferably in the PaaS model, from a MeitY empanelled cloud service provider in a managed services model. The MSI will also be responsible for installation and commissioning of solution components on provisioned infrastructure.

- **Software Operations and Maintenance:** The MSI shall be responsible for the maintenance of all technology components developed, which includes but not limited to bug fixes, patch upgradation, performance optimization, etc. The MSI should aim to utilize the latest version, or previous versions (in case of stability issues in latest version) of software. In case, the MSI requires exemption from this, the MSI should request the CHiPS for such an exemption giving clear reasons for this request.

- **Provisioning of Licenses:** The MSI needs to provide necessary software licenses, along with their enterprise support, to meet the performance and scalability requirements. The licenses need to be unrestricted and perpetual in the name of CHiPS. The MSI will have to propose products (COTS/ Open source) mentioned in the concerned benchmarking reports (Leaders/ Visionary/ Major players/ strong performer Quadrant/ wave of Gartner/Forrester/IDC). For specific product criteria is listed in Annexure-III.

- **Onboarding of schemes and departments:** The MSI will be responsible to onboard 5 shortlisted schemes on IPeG as part of track 2. This will be followed by onboarding of 45 schemes as part of track 3. Onboarding has been defined as follows:

Requirement Gathering	Onboarding of Toolkits	Onboarding of Platform Services	UAT and Training
Initial Five (5) Schemes			
Current State Assessment, Requirement Gathering, etc.	All the toolkits need to be configured and integrated with scheme. *Note: For toolkits, which are not required by the scheme, the MSI will need to obtain a declaration from concerned department and CHiPS*	All the platform services need to be configured and integrated with scheme. *Note: For platform services, which are not required by the scheme, the MSI will need to obtain a declaration from concerned department and CHiPS*	Obtain UAT sign-off for all toolkits and platform services. Conduct end-user trainings as per the training calendar finalized in consultation with the respective department and CHiPS.
Other Forty-Five (45) Schemes			
Current State Assessment, Requirement Gathering, Identification of required toolkits and platform services, Government Process Reengineering, etc.	All the toolkits required by the department needs to be integrated/configured for the given schemes *Note: For toolkits, which are not required by the scheme, the MSI will need to obtain a declaration from concerned department and CHiPS*	All the platform services required by the department needs to be integrated for the given schemes *Note: For platform services, which are not required by the scheme, the MSI will need to obtain a declaration from concerned department and CHiPS*	Obtain UAT sign-off for all required toolkits and platform services. Conduct trainings to master trainer(s) as per the training calendar finalized in consultation with the respective department and CHiPS.

- **Training and Documentation:** The MSI will be responsible for requisite training on operation, maintenance, handholding, etc. The functional support and coordination will be carried out by the CHiPS in-house team and MSI will be required to provide them necessary trainings and documentation.

- **Knowledge transfer and End of Contract** - Knowledge transfer needs to be initiated 3 months prior to stipulated end time of project. A detailed knowledge transfer plan needs to be submitted prior to that and a sign-off needs to be obtained from CHiPS

3.2. Detailed Scope of Work

3.2.1. Toolkits

3.2.1.1. Toolkits – Scheme Analysis and Policy Planning Tool

The Policy Planning Toolkit is envisaged to be a centralized tool which will help the departments in designing of new schemes, budgeting and rationalization of existing schemes, and monitoring of existing schemes. Within the Policy Planning Tool, the departments will be able to apply different criteria to identify potential beneficiaries for new schemes, identify potential beneficiaries in existing scheme which are yet to be enrolled and proactively reach out to them, etc. The Policy Planning Tool will be able to access the data in the social registry through the Data Exchange Gateway. However, the Policy Planning Tool will not obtain any personal information of the resident, and the data will be shared with the Policy Planning Tool in an anonymized or deidentified manner. In addition, there should be a facility for the departments to upload their own data for analysis on this tool. The MSI can aim to leverage the advance analytics tool or provide any specific tool for implementation of this toolkit.

The requirements are explained in a summarized manner below and for more details, please refer to Annexures.

S No	Objectives	Description
1.	Scheme Design	▪ Historical data about the beneficiaries can be analysed and insights from the analysis can be used to conceptualize and formulate new schemes/programs in the state. The information which may be used to design new schemes using the policy planning tool may include: ▪ Geographical spread ▪ Age distribution ▪ Socio Economic parameters (Income Level, Disability Status, Poverty Indicators, Occupational Status, Any other data field available with departments) ▪ Departments should be able to create multiple scenarios of beneficiary count/beneficiary list by changing selections for the different data fields (option to select different subsets of data for different data fields). ▪ Department users should be able to define a scheme along with its eligibility conditions and should be able to know how many beneficiaries in the database would be eligible for receiving the benefit under the defined scheme. o What-If Analysis – Policy Implication Modelling should also be there in the proposed tool. Like - Impact of change

S No	Objectives	Description
		in the selling price for a service, Impact of removing a service.
2.	Scheme budgeting and rationalization	The policy planning tool should be able to be used for scheme budgeting and rationalization. This can be done by creating different scenarios. For example, to design a new scheme/program the policy makers may want to evaluate various scenarios – such as how should they define the eligibility conditions to achieve the target number of beneficiaries, how should they define the eligibility conditions to give certain minimum monetary benefits to the beneficiaries, how should they define the eligibility conditions and identify the target population such that a defined budget is not exceeded and so on. Policy makers, using the tool, should be able to design and evaluate different scenarios the and arrive at the optimum set of eligibility conditions to design a new scheme/program.
3.	Monitoring and analysis of existing schemes	Department users should be able to monitor the existing schemes running in the state by creating various reports and dashboards for KPIs and key data fields based on beneficiary data/scheme implementation data available with them. The policy maker should be able to schedule reports, dashboards and alerts based on time/occurrence of an event etc. The Proposed solution should also have capabilities to perform: – Beneficiary Eligibility Validation (Age, Income, gender, and other parameters) – Automated List generation for new schemes – Inclusion/ Exclusion of beneficiaries – Duplicate Beneficiaries – Cross Scheme Level Analysis
4	Scheme Efficiency & Efficacy	– Analyse operational performance of schemes – Fund allocated vs financial progress of schemes – Scheme Sub-SLA Monitoring

For the above purpose, CHiPS has planned to provide a Policy Planning Tool is required to be provided to the departments of Government of Chhattisgarh. Initially, the access to Policy Planning Tool will be provided to the selected department users which are technology savvy. In addition, the software for Policy Planning Tool will be utilized to generate reports, basic analytics,

etc. for which additional users are planned. Some key functional requirements are specified below:

S. No.	Requirements
Create and Manage User Profiles	
1.	**Create and Manage User Profiles** • The Super admin and Department admins should be able to create/add/delete users. • The Super admin and Department admins should be able to manage user profiles.
2.	**Provide role-based access** • The Super admin and Department admins should be able to assign role-based access rights to the user using the principle (create, read, update, delete).
Data Management	
3.	**Numerous Data connections** • The Department Technical Users should be able connect the tool to varied data sources, both online and offline, without any programming. Notable connectors include Cloudera Hadoop, SQL Server, MongoDB, PDF files, Excel files, CSV, APIs etc.
4.	**ETL Management and Data Processing** • The Department Technical users should be able to enhance, refine, or prepare raw data for analysis using an inbuilt/integrated ETL tool. • Data Quality –Department Technical users should be able to assess the quality of data being ingested in the tool. • Data Cleaning –Department Technical users should be able to refine, enhance and clean data tables during data ingestion phase. • Automated data refresh –Department Technical users should be able to automate the data ingestion and cleaning process. These users should be able to configure the refresh period.
5.	**Data Label management** • The Department Technical users should be able to manage the labels of different data fields on the portal/ tool.
6.	**Cross Database/Table integration** • The Department Technical users should be able to integrate different tables and databases

S. No.	Requirements
	both structured and unstructured to generate an integrated data set for the purpose of reports and dashboards. • The Department Technical user should also be able to save data table created for the reports for later use.
Insight Generation – Data Operations, Data Analysis (Dashboards/Reports Creation), Scheme Design/Budgeting and Rationalization	
7.	**Data Operations** • **Data field creation:** The design users should be able to create new data fields by applying formulas/concatenating existing data fields. • **Data Processing** – The design users should be able to refine, enhance and clean existing data tables for creating reports and dashboards.
8.	**Data Analysis (Dashboards/reports creation)** • **Create Dashboards**: The design users should be able to create their own dashboards via a simple drag and drop mechanism to analyze the historical beneficiary data and to monitor existing schemes. The dashboards would contain different reports/charts/graphs that user may decide to have. • **Create different types of visual representations (Visual Discovery):** The design users should be able to change representation layout and visual formatting on the charts/graphs (e.g. sunbursts, bars, columns, radial bars, maps etc.). They should also be able to add texts, images, icons on the chart and also back-up, redo and undo work. • **Custom Visual Imports:** The design users should be able to import custom visuals from the Web. • **Create Geospatial Representation:** The design users should be able to show geographical data on a map. • **Predefined Templates:** The design users should be able to use various pre-built templates to create reports and dashboards.
9.	**Scheme Design** • Design users should be able to create multiple scenarios of beneficiary count/beneficiary list by changing selections for the different data fields (option to select different subsets of data for different data fields). • Design users should be able to define a scheme along with its eligibility conditions and should

S. No.	Requirements
	be able to know how many beneficiaries in the database would be eligible for receiving this benefit under the defined scheme.
10.	**Scheme Budgeting and Rationalization** • The policy planning tool should be able to help undertake scheme budgeting and rationalization. This can be done by creating different scenarios. For example, to create a scheme the design users should be able to evaluate various scenarios – such as how should they define the eligibility conditions to achieve the target number of beneficiaries, how should they define the eligibility conditions to give certain minimum monetary benefits to the beneficiaries, how should they define the eligibility conditions and identify the target population such that a defined budget is not exceeded and so on. Design users, using the tool, should be able to design and evaluate different scenarios and arrive at the optimum set of eligibility conditions to design a new scheme/program.
View and Update Reports/Dashboards	
11.	**View dashboards and reports** • The Administrative users should be able to view multiple reports and dashboards shared with them by different design users in separate tabs. • The Administrative users should be able to integrate multiple reports and dashboards on a single screen/window/tab. • The Administrative users should be able to seamlessly toggle between different tabs to view dashboards.
12.	**Filters and drill downs** • The Administrative users should be able to filter, slice/dice, and drill up and down at speeds that make it possible for them to delve into huge volumes of data (refer list of a few filters in the next section on 'Features').
13.	**Review and provide comments on reports/dashboards** • The Administrative users should be able to add texts/ comments/ questions / observations on the chart and/or in a separate section on the dashboard.
Dashboard Visualization Features	

<table>
<tr><th>S. No.</th><th>Requirements</th></tr>
<tr><td>14.</td><td>
<table>
<tr><th>Features</th><th>Description</th></tr>
<tr><td>Click-to-Filter</td><td>This allows dashboard users to utilize the dimensions of the dashboard’s charts and graphs as temporary filter values</td></tr>
<tr><td>Drilldowns</td><td>This shows the user more specific, and detailed information of an element, variable or KPI, without overcrowding the dashboard. (5 level of drill downs should be available)</td></tr>
<tr><td>Time Interval Widget</td><td>This allows the user to enhance individual time scales on different charts on dashboards with an interactive drill-down function</td></tr>
<tr><td>Chart Zoom</td><td>This function would let users to drill-down into the smallest unit of data represented in charts/graphs. Chart zoom would allow users to simply drag the mouse over the part of the chart they wish to view on a more granular basis.</td></tr>
<tr><td>Custom Chart Tooltips</td><td>This option enables users to adjust the shown information when they hover over with their mouse providing a small snippet.</td></tr>
<tr><td>Show or Hide Chart Values</td><td>This feature helps the user better manage blended data. With a show or hide chart values feature, charts containing more than one dataset are presented with a dynamic legend at the bottom.</td></tr>
<tr><td>Dashboard Widget Linking</td><td>This enables the users to add links to any widget on their dashboard whether it’s a chart, textbox or image and redirects dashboard users and viewers to other related content. They may link to another dashboard tab or even to an external website or resource.</td></tr>
<tr><td>Conditional Formatting</td><td>It lets users highlight variances to point out unexpected values and discover hidden trends and patterns. e.g. heat maps</td></tr>
</table>
</td></tr>
<tr><td colspan="2">Other Features</td></tr>
<tr><td>15.</td><td>Report Scheduling
All design and administrative users should be able to schedule reports and dashboards based on time/occurrence of event(s)/crossing of thresholds.</td></tr>
<tr><td>16.</td><td>Save and share</td></tr>
</table>

S. No.	Requirements
	• All design and administrative users should be able to save the reports/dashboards/comments / texts on the portal/tool and to a local PC/ Laptop. • **All design and administrative users should be able to share the dashboards / reports/comments / texts with other users on a real time basis over the tool/portal and email.**
17.	**Exporting and Printing Capability** • **Export Reports:** All design and administrative users should be able to export the data or report to spread sheets, including graphics /observations/ comments /texts into flat file, csv, pdf, xls, html formats etc. • **Print Reports:** All design and administrative users should be able to directly send the report for printing on a LAN printer / personal printer.
18.	**Dashboard rotation and full screen options** · All design and administrative users should be able to view the dashboard on a full-screen mode and toggle between normal and full-screen mode users should be able to receive/send alerts, over web, on the network (email) and on mobile devices.
19.	**Cross-Device Accessibility** · All users should be able to access the tool on different devices e.g. mobile, tablet, PC etc.
20.	**Notification** · All users should be able to receive/send alerts, over web, on the network (email) and on mobile devices.

The MSI shall be responsible to ensure integration, including but not limited to:

- **Supply, Installing, Commissioning of IT Software Systems:** MSI is responsible for sourcing, installing and commissioning of the Software Systems for Policy Planning Tool on its own cloud infrastructure in PaaS model (preferable), or SaaS model.

- **Software Customization or Integration:** MSI shall be responsible to ensure integration, including but not limited to:
    - Data related services i.e. Fetch Data, Data Anonymization and Data Identification to obtain the required data

- Integration with Common Services Portal, Mobile Application, State DBT Portal, etc. for publication of dashboards

- **Software Operations and Maintenance:** The MSI shall be responsible for the maintenance of the Policy Planning Tool which includes but not limited to bug fixes, patch upgradation, etc.

- **Provisioning of Licenses:** The MSI will be responsible for providing licenses for 10 department users, 2 CHiPS users, and 3 CHiPS tools related users. CHiPS may place orders for additional licenses at the discovered rates, as necessary.

- **Training:** The MSI will be responsible to training to the per department users (no. 15) and CHiPS users (nos. 10). MSI shall be responsible for ensuring all the users of Policy Planning Tool are adequately trained to work on the tool to meet the objectives. In case additional licenses are procured there will be a need to train the new users, for this purpose MSI will train the CHiPS staff to fulfil the responsibility of master trainers. Thus, MSI will be required to do (i) Training need assessment, (ii) prepare training plan and content, and (iii) impart trainings and ensure its effectiveness.

- **Handholding support for provisioned licenses:** The bidder shall also be responsible to provide technical support to the departments onboarded on the IPeG platform and are using the Policy Planning Tool. The support required to be provided by MSI is as follows:
  - **Business Services**
    - Data Access Management (Coordination with CHiPS team for access to data sources)
    - User Management services (support in creation, modification and removal of roles and users)
  - **Technical Services**
    - Data source management (access permissions, data schema and data quality analysis, installation, configuration and troubleshooting of connectors at the data sources)

3.2.1.2. Toolkits – Data Collection Tool

This toolkit will enable the government official to collect the data either as part of their existing service record or as a fresh record.

As part of the end-to-end digitization, there will a requirement of digitization of existing manual data (on paper-based record books), cleansing of electronic records (on excel sheets) and cleansing of existing electronic data (on databases). The no. of data attribute for centralized fields are mentioned in Annexure however, Decentralized data fields will be informed latter (which maybe approximately 60-120 of data fields). The toolkit will provide the data entry interface with built-in validations and data approval process to ensure that the digitization exercise results in a high-quality data. This interface will allow for entry of records in a singular manner as well as bulk

mode. Upon loading of the data in the toolkit, CHiPS will assist the department to conduct the data quality assessment to identify data quality gaps.

Once the gaps are identified by the departments, the department may want to collect this information from the residents. MSI will configure the toolkit which will enable the field officials to fill the data gaps using their mobile phones, enabling real-time data validations and ensuring data quality. Once the data is captured, the toolkit may be configured for data quality assurance process.

Key Functional Requirements are as below:

S. No.	Requirement Title
Data fields to be collected should be configurable as per need of the department	
1.	**Purpose** Every department who is provided with the survey tool will need to configure it as per the data quality requirements and the data fields, documents that need to be collected, so that the tool can be readied for the survey **Actors** • Technical staff of department • Technical staff of CHiPS **Inputs** • User and their roles submission • Data fields that must be collected • Define documents that must be collected • Define the validation process of data fields and documents • Define the different dashboards **Processing** • Once all inputs have been provided, the system will be auto-configured as per the provided inputs • A message would pop up stating that tool configuration is successful • In case there are any errors, it should be visible with the exact cause of error **Output** • A ready to use tool where enumerators can log in and conduct the survey. • The data collected will be visible to different user roles depending upon how it was configured

S. No.	Requirement Title
It should have in-built feature of Aadhaar authentication (OTP, Biometric & Demographic modes)	
2.	**Purpose** The tool should be able to help enumerators to authenticate themselves as well as authenticate the resident being surveyed. Aadhaar based authentication is fool proof, hence this tool should enable the 3 most commonly used modes of authentication viz. OTP, biometric and demographic **Actors** • Department Enumerator **Inputs** • Aadhaar number and biometric of the resident **OR** Only Aadhaar number **OR** Virtual ID • Mode of authentication will be selected (OTP/Biometric/Demographic) • Type of request (Auth/e-KYC) • Electronic consent **Processing** • Once inputs are provided, it should send request to the designated Authentication User Agency of CHiPS • Consent is stored in the system **Output** • On basis, mode of authentication selected, the output will depend. • Output will only be a yes/no if it is a simple auth request • Output will have all fields present on Aadhaar card if there is e-KYC request • In case of an OTP mode of authentication, number will be routed to the registered mobile number, which when input in the tool, authentication would be a success • If authentication is successful, then Aadhaar number along with the consent obtained would be stored in the system
In-built feature of Bank account details authentication (Account no., Branch name, Bank name) and linked with NPCI mapper to detect whether bank account is linked with Aadhaar	

S. No.	Requirement Title
3.	**Purpose** To ensure error free payment disbursals, it is required to verify the bank account details shared by the resident. Additionally, to enable Aadhaar based payments, Aadhaar linking to bank account should be diagnosed at the time of data collection **Actors** • Department Enumerator **Inputs** • Bank account holder's name • Bank account number • IFSC code • Branch name • Aadhaar **Processing** With the details input, the system should check the data with the bank master and check with the NPCI mapper **Output** • It should retrieve the customer details present against the input fields provided • It should return a Yes/No for seeding status in NPCI mapper against the bank account details provided
It should have in-built feature to verify mobile number through OTP	
4.	**Purpose** In order to ensure resident receives regular updates on application status of their services or schemes applied, to get feedback on service and to facilitate easy lodging of grievances, correctness of mobile number is required, and it is necessary to establish that mobile number provided belongs to the resident being surveyed **Actors** • Department Enumerator **Inputs** • Mobile Number

S. No.	Requirement Title
	Processing • The system should hit an OTP engine and generate an OTP that is sent to the provided mobile number • An OTP will be generated and sent to the mobile number provided during the survey **Output** The OTP is then keyed into the system, if successful then the mobile number should be collected and stored
5.	**Purpose** It should enable uploading of documents, photographs, audios and videos as per requirements of department **Actors** • Department Enumerator **Inputs** • Document scan • Photograph • Audio • Video **Processing** • The system will give upload options with a link • On successful upload, a message will be displayed • On upload failure, a message will be displayed with reason of failure **Output** Document/Audio/Video/Photograph will be uploaded with a thumbnail or a link as per established UI/UX standards
It should support GIS enabled geotagging of data collected as per requirements of department	
6.	**Purpose** GIS enabled tool will enable to monitor the locations of enumerator as well as the geo-tagged data needs to be collected for service delivery, monitoring and reporting purpose

S. No.	Requirement Title
	Actors • Department Enumerator **Inputs** • Data records • Photograph of physical assets like land or property • GIS or Geo-tag of the data fields **Processing** The input fields would be consumed by the application **Output** Verified Geo-tagged data records
It should be compliant with Local Government Directory (LGD) and enable collection of address as per LGD codes	
7.	**Purpose** Collection of beneficiary address needs to be undertaken in a standardized format. Government of India has standardized codes and template which has been suggested to store address in database. The survey tool should therefore be compliant with it. **Actors** • Department Enumerator **Inputs** • Dropdown which will have LGD compliant addresses & codes • Text entered for details like apartment number and house number **Processing** • The system will consume the resident address and run it through pre-configured front-end validations • It will display message “address updated successfully” if all data is entered as per set protocols

S. No.	Requirement Title
	• It will display message “address update failed” along with the error in case address is not absorbed by the system **Output** Updated address of resident in compliance with LGD
It should support uploading of databases at the backend, prior to survey	
8.	**Purpose** Departments may need to improve the quality of their existing database through survey. In order to do so they will have to upload the database to the survey tool so that they can have pre-filled data fields that can be edited on field based on information provided by department beneficiary. **Actors** • Department Enumerator **Inputs** • Database uploaded to the tool • Pre-filled data fields visible to the enumerator **Processing** • Each of the data fields open up one by one for the enumerator with pre-filled entries fetched from the existing database • On basis of information and supporting documents received during survey, the enumerator edits the existing data fields • The edited data fields should also abide by pre-defined data validations and if there is a violation, the system should throw an error message • If the data fields are successfully updated, then it should display a message “data updated successfully” • In case data fields are not updated due to some error, a message should be displayed “error in data update” along with the exact reason for error • In case of pre-filled null entries also, new data will be entered in compliance with pre-determined validation rules **Output** Department will have error free updated database
It should support dashboard or report features	

S. No.	Requirement Title
9.	**Purpose** After data is collected by the enumerator or also intermittently when data is being collected through a survey, survey supervisor or other officers of the department would need to review the quality of data being collected. **Actors** • Department survey supervisors, Functional user of the department or head of the department **Inputs** • Data filters or Data queries to fetch data that has been collected • Type of data representation wanted • User role **Processing** • The level of processing will depend on the defined inputs. • Data fetch and representation will depend on the queries and filters applied **Output** • Raw data sample queried for sample check • Data representation or dashboard or report of data collected
It should have facilities to send message/ notifications/ data samples from one user to the other user	
10.	**Purpose** After review of data collected, head of the department, a functional authority of the department or survey supervisor might not be satisfied with the quality of data collected. In this scenario, they should be able to send back the sample data with remarks to the user for necessary correction **Actors** Department survey supervisors, Functional user of the department or head of the department who will initiate the message or notification and Enumerator who will act on the notification or message sent **Inputs** • Sample data or data representation with errors or incompleteness or inconsistencies • Message body

S. No.	Requirement Title
	Processing The message along with data sample would be relayed by the system **Output** • Message & Notification with sample data source/ data representation which was checked • Corrected data and return message or notification
11.	Few of the sample cleaning activities that proposed solution should have: • Data Quality for checking quality of data before it goes for record creation within the Repository • Check for the completeness and accuracy of the data and highlight any exceptional records. • Solution should be capable of carrying out de-duplication process to detect any duplicates within the data. E.g. Fuzzy demographic matching to find the duplicate enrolment requests to make sure the data is clean before it is sent for Applicant Master Record Creation • Solution should have capabilities around anonymization (masking of PII information of citizen) & de-identification of data to ensure that privacy of citizens is maintained. • The proposed solution should support data quality measurement on an on-going basis embedded into batch/ near-time • The proposed solution should have the capability to enrich data from external/third party data sources • The proposed solution should have transformations to perform analytical operations like Correlations, Distribution Analysis, Frequency and Summarization. • The proposed solution shall have the capability to correct mistakes in spellings, inconsistencies, casings and abbreviations • The proposed solution shall support correction logic for Indian names, addresses, phone numbers, pan numbers, passport number and other identification proof documents and demographic details • The proposed solution shall support profile matching through multi-field text matching functionality on beneficiary-profile information (comparison could be on combination of name, PAN, address, telephone number etc.)

The MSI shall be responsible to ensure, including but not limited to the following:

- **Solution Design:** The MSI will be responsible to gather the detailed requirement for this toolkit and prepare the detailed design for this component. The design should cover various usage scenarios, ability to configure through simple drag-and-drop, integration with internal and external components for data fetching and data validation, etc.

- **Supply, Installing, Commissioning of IT Software Systems:** MSI is responsible for sourcing, installing and commissioning of the Software Systems for Data Collection Tool on its own cloud infrastructure in PaaS model.

- **Software Customization or Integration:** MSI shall be responsible to ensure integration, including but not limited to:
    - Data related services i.e. Fetch Data, Data Anonymization and Data Identification to obtain the required data
    - Integration with Common Services Portal, Mobile Application, State DBT Portal, etc. for publication of dashboards

- **Software Operations and Maintenance:** The MSI shall be responsible for the maintenance of the tool which includes but not limited to bug fixes, patch upgradation, etc.

- **Provisioning of Licenses:** The MSI will be responsible for provide unrestricted and perpetual licenses for all data collection exercises to be carried out by the departments. Thus, the license requirements should not be restricted by the number of end-users.

- **Training:** The MSI will be responsible to training to the master trainers of CHiPS. MSI shall be responsible for ensuring all the master trainers are adequately trained to train the end users enabling them to work on the tool. MSI will be required to do (i) Training need assessment, (ii) prepare training plan and content, and (iii) impart trainings and ensure its effectiveness.

- **Handholding support to department:** The MSI shall also be responsible to provide technical support to the departments onboarded on the IPeG platform and are using the Data Collection Tool. The support required to be provided by MSI is as follows:
    - Configuration of data fields on the data collection tool
    - Configuration of workflow for approval process on the data collection tool
    - Configuration of concerned users for data entry/collection, data verification, etc. on the data collection tool
    - Undertake data quality assessment of existing database, if any, to identify the gaps in data quality
    - Integration of existing database, if any, for which the gap data collection is required with the data collection tool

3.2.1.3. Toolkits – Service Delivery Application

This toolkit will enable the government departments in rapid digitization of scheme delivery workflow. This will be a low code, no code tool that has in-built tools/interfaces for designing, configuring and executing scheme delivery. The MSI can undertake rapid configuration and customizations for the line department on basis of detailed workflow details provided viz. the manual application form, the approval authorities, the validations or parameters on basis of which

an application is approved, the output document or instructions that need to be communicated to an external system.

MSI will configure the toolkit as per custom requirement of the department using features like drag and drop form designer, custom notification designer, document designer. Additionally, this tool will support easy API based integration with other state government systems and central government systems like Digilocker, Public Financial Management System etc. It will have capability of producing basic MIS reports on transactional data and should be able to share data with third party BI tool for advanced representation and analytics. The applicant and authorities should be able to track the status of their applications and receive periodic notifications on status of their application or applications that require their action.

Some Key Functional Requirements are as below:

S. No.	Requirement Title
User Authentication	
1.	Ability for users of the system to authenticate themselves for the purpose of signing in through SSO solution developed for IPeG. Feature to login using external sources (e.g. external active directory)
Scheme Configuration	
2.	Low/ no code tool which departments can use to configure and deploy schemes
3.	Configure & Deploy DBT schemes/regulatory/statutory/ utility services
4.	Create/Edit/ Manage multiple service categories
5.	Custom design output documents (certificates)
Application Form Configuration	
6.	**Authentication** • Aadhaar Authentication (Demographic/Biometric/Offline/e-KYC) – Enabled through integrated with State's Aadhaar Authentication Infrastructure • Non-Aadhaar Authentication - Accept other forms of electronically (e.g. Ration Card) or manually (e.g. Passport, PAN Card, etc.) verifiable identity, pass authentication request to an officer and upon his approval mark the person as identified

S. No.	Requirement Title
7.	**Auto-fetch data/documents from internal/external database** • Information for certain fields/documents to be auto populated/fetched through internal database and external data sources (to be accessed through APIs via a data exchange platform) based on business rules defined. Information/documents to be fetched from databases of external IT systems of GoI/GoCG. • In case the external systems are not responsive at the time of application, allow those specific data fields to be filled after submission of form but before it is taken up for approval • Fetch documents from Digi-locker to verify document authenticity and push documents created into Digi locker through informed consent of the user • This feature of auto-fetch needs to be built into the custom controls of the data fields. The data fields on application form should be intelligent and can be configured to have an auto-fill option based on business rules (invoke APIs, scripts etc.)
8.	**Trigger requests for another service within/outside Tool** Ability to trigger workflow for another service (within/outside Tool systems) on some conditions being met (based on business logic): • continue processing the application and separately initiate the application of new service • put the process of current application on hold till the time response is received from new services triggered, and have ability to consume response of additional workflow
9.	**Trigger requests for another service within/outside Tool** Ability to trigger workflows in series and parallel and feature to have response of one service to act as input for another service.
10.	Checking of Aadhaar linking status with bank account by integration with NPCI service *(National Social Assistance Platform developed by Central NIC offers this feature*)
11.	**Mechanisms to verify data/ document provided by applicant** • Avail standard online mechanisms for data verification viz. Aadhaar OTP based authentication, demographic authentication, bank details verification • Provide department option to configure any other machine-based verification mechanisms as per needs of the service/ scheme to be delivered

S. No.	Requirement Title
	• Upload scanned images or documents in accordance to verification protocols set by a department

12.	**Other general features**
	• Bi-lingual application form generation
	• Feature to write custom validation (static and dynamic) for data fields in the application form
	• Auto-saving of:
	  o Form and allowing the user to edit it later
	  o Each page in case of multi-page form
	  o Fields in case of new form being opened
	• Allow the user to continue from last activity onwards

Workflow Configuration	
13.	Define workflows & assign workflow roles
14.	Ability to verify data (by reviewers/approvers) which has been manually entered, fetched from internal system(s) and external system(s)
15.	Ability to read and verify (by reviewers/approvers) certificates fetched from internal system(s) and external system(s)
16.	Define timelines against each role, user for a task & activate auto-escalations
17.	Support forking of workflows in series and parallel
18.	Design notifications and define when they need to be sent, both inside and outside tool environment
19.	Provide status of application at different stages of workflow
Payment Processing / Acceptance	
20.	Compute benefit amount based on beneficiary DBT details & scheme benefit information provided by department

S. No.	Requirement Title
21.	Enable DBT payment through PFMS for schemes onboarded on Service-Plus platform Create and transfer XML based payment files to external systems/ SFTP servers (for e.g. PFMS) PFMS requires digitally signed XML payment files to be transferred through SFTP servers for PFMS consumption
22.	Enable DBT payment through PFMS for schemes NOT onboarded on Tool platform. These schemes would use Tool for the functionality 'DBT Payment through PFMS'
23.	Fetch reconciliation status from external system (e.g. PFMS) and utilization status from external systems
24.	Send data on utilization of funds disbursed to beneficiaries to external system so that it can mark them as utilized (e.g. data to be sent to PFMS of GoI/IFMIS of GoCG)
25.	Accept different modes of digital payment viz e-wallets, payment gateways: • Accept payment through e-wallets (e.g. CSC wallet, wallets offered by banks, other financial sector companies) • Accept payment through different payment gateways (in assisted or self-service mode) • Hold application for want of payment (don't have sufficient funds) or confirmation (manual challan)
26.	Configure logic for payment distribution in multiple heads
27.	Create MIS reports on payment collected by service, channel, mode of payment, Service Delivery Center, District etc
28.	Feature for user departments to accept bulk payments via payment gateways from other Government offices/departments in case service fee burden is waived off from the resident and is to be borne by a government department or any other government implementing agency
Analytics / MIS Capabilities	
29.	Should have the capability to create different kinds of dashboard/ reports as per business needs at Department/District/ Sub-District levels

S. No.	Requirement Title
30.	Should have the capability to show transactional data, aggregate data on beneficiary management aspects and payment reconciliation
31.	Should have drill down capabilities, for e.g. users can drill down from state -> district -> tehsil ->block -> panchayat -> village to gauge the penetration of a service/ scheme
32.	Other real time monitoring capabilities, user role wise, service/scheme wise, administrative area wise. Includes ranking capabilities based on set criteria
Data Exchange with Other Systems	
33.	Push/ Fetch & Pull data from/ to other systems via APIs
34.	At the time of application submission for a scheme a) On this BPM Solution – Fetch data from other services (within/outside this BPM solution) b) On other IT systems – Push data (from one of the services on Tool) via APIs as required by other IT systems
35.	Trigger based push/pull data to/from other schemes (within/outside this BPM solution)
36.	Share data for data analytics and policy planning
37.	Other use cases of exchange of data basis the needs of different departments
38.	• IPeG Platform and its platform services • Policy planning tool developed IPeG Platform • Existing/Upcoming IT systems used by departments of Government of Chhattisgarh • Data Exchange Platform of IPeG (to be built – will enable exchange of data across systems/departments governed by Data Exchange Guidelines) • Digi-Locker • UIDAI through AUA/ASA • NPCI • PFMS of GoI/ IFMIS of GoCG • Other GoI Systems like e-Taal, RAS, Darpan etc.

S. No.	Requirement Title
	• Payment gateways or digital payment acceptance platforms • CSC Platform
General Features	
39.	System should be able to consume platform services to be built on IPeG Platform
40.	System should have audit trail (telemetry)

The MSI shall be responsible to ensure, including but not limited to the following:

- **Solution Design:** The MSI will be responsible to gather the detailed requirement for this toolkit and prepare the detailed design for this component. The design should cover various usage scenarios, ability to configure through simple drag-and-drop, integration with internal and external components for data fetching and data validation, etc.

- **Supply, Installing, Commissioning of IT Software Systems:** MSI is responsible for sourcing, installing and commissioning of the Software Systems for Service delivery application on its own cloud infrastructure in PaaS model.

- **Software Customization or Integration:** MSI shall be responsible to ensure integration, including but not limited to:
    - Data related services i.e. Fetch Data, Data Anonymization and Data Identification to obtain the required data
    - Identity authentication and data validation services
    - Messaging service, payment through PFMS service, Publish document to Digilocker service etc.
    - Integration with Common Services Portal, Mobile Application, State DBT Portal, etc. for publication of dashboards

- **Software Operations and Maintenance:** The MSI shall be responsible for the maintenance of the tool which includes but not limited to bug fixes, patch upgradation, etc.

- **Provisioning of Licenses:** The MSI will be responsible for provide unrestricted and perpetual licenses for all service or scheme digitization exercises to be carried out by the departments.

- **Training:** The MSI will be responsible to training to the master trainers of CHiPS. MSI shall be responsible for ensuring all the master trainers are adequately trained to train the end users enabling them to work on the tool. MSI will be required to do (i) Training need

assessment, (ii) prepare training plan and content, and (iii) impart trainings and ensure its effectiveness.

- **Handholding support to department:** The MSI shall also be responsible to provide technical support to the departments onboarded on the IPeG platform and using the Service delivery application. The support required to be provided by MSI is as follows:
  - Configuration of multilingual (English & Hindi) forms as per the manual application form of a scheme, which would also include the front-end and back-end validations for each field in the form. This may also require invoking of platform services, which need to be integrated through APIs
  - Configuration of the approving authorities, approval workflow for an application. In case of workflow complexities minor coding effort may also have to be undertaken
  - Configuration of notifications or messages that need to be sent to different stakeholders during application processing
  - Configuration of output document or payment instructions that need to be passed on to third party systems for completion of scheme delivery
  - Integration with platform services and third-party platforms as per IPeG project requirement and line department specific requirement

3.2.1.4. Toolkits – Grievance Management Tool

The grievance management tool will be used to manage all grievances relating to public service delivery across the state of Chhattisgarh. This module will be used to lodge grievances, notify relevant government departments of new grievances, manage SLAs and provide for escalations for SLA breaches for existing grievances. This module can be configured by respective departments with help from MSI as per need basis. The MSI can aim to leverage the service delivery application for this purpose or provide an open source tool for implementation of this toolkit.

The tool should support the functionalities outlined below: -

a. API based integration with authentication related platform services and data related platform services

b. Lodging and tracking of grievances for schemes onboarded using service delivery application of IPeG

c. Assigning grievances to competent authorities and digitizing workflow between different levels of appellate authorities, along with SLAs, list of action required etc.

d. Configure forms and attachments for raising grievances

e. Omnichannel access enabled for the appellate authorities to investigate the grievances raised and provide a timebound resolution

f. Support messages or alerts that can be sent to the appellate authority when a new grievance has been assigned to them or the

g. Basic reporting and analytics on the grievances raised, pending closure, time taken for closure etc.

Some key functional requirements are specified below:

S. No.	Requirement Title
User Authentication	
1.	Ability for users of the system to authenticate themselves for the purpose of signing in through SSO solution developed for IPeG. Feature to login using external sources (e.g. external active directory)
Lodging Grievances	
2.	The resident should be able to input the grievance in the below mentioned methods • Online – Can be lodged anytime using any of the access channels • Offline – Can be lodged by sending a letter, or an email to the District Grievance Nodal Officer (DGNO).
3.	**Authentication** • The resident should be able to authenticate themselves using Aadhaar Authentication (Demographic/Biometric/Offline/e-KYC) methods – Enabled through integration State's Aadhaar Authentication Infrastructure • The resident should be able to authenticate themselves using Non-Aadhaar Authentication methods - Accept other forms of electronically (e.g. Ration Card) or manually (e.g. Passport, PAN Card, etc.) verifiable identity, pass authentication request to an officer and upon his approval mark the person as identified

S. No.	Requirement Title
4.	**Application** • The resident should be able to lodge the grievance using the Receipt ID generated for a public service using IPeG. • The resident should be able to lodge a grievance without Receipt ID by selecting department and the scheme or service in drop down menus • The resident should get an exhaustive list of possible grievances to choose from in drop down menus. • The resident should get the option of manually entering the grievance in a dialogue box. • In case the resident needs to argue an incorrect denial of application, he/she should be able to fetch relevant information by providing Aadhaar number through data exchange platform.
5.	Once lodged, there should be a tracking number provided to the resident to follow up on the status of the grievance.
6.	The user should be able to file and track complaints through any smart phone
7.	**Geospatial features** • The tool should have Integration to provide support for attaching photos and integration with Maps • The user should be able to geo-tag images
8.	**Reporting and analytics** • The user should be able to generate insights and reports from the tool • The user should be able to integrate the tool with advanced business-intelligence and analytics tools
9.	**Data Exchange** • Push/ Fetch & Pull data from/ to other systems via APIs • Share data for data analytics and policy planning • Other use cases of exchange of data basis the needs of different departments

S. No.	Requirement Title
Other general features	

10.	• Bi-lingual application form generation
	• Auto-saving of:
	  ○ Form and allowing the user to edit it later
	  ○ Each page in case of multi-page form
	  ○ Fields in case of new form being opened
	• Allow the user to continue from last activity onwards

Processing in detail	
11.	**ONLINE:** The processing of the request will be based on the input received. 1. ***When the input is the Receipt ID*** – User can lodge a grievance using the Receipt ID, in self or assisted mode: *Self-mode:* The user will log in to the IPeG portal and navigate to the grievance module. The user will enter the Receipt ID for which the grievance management ticket is to be raised. The user will find a list of possible grievances (dropdown) and an option to type a grievance in a dialogue box. *Assisted mode*: The user will visit CSC/LSK/CHOiCE or Government Office or call the Call Centre number to lodge a grievance using the Receipt ID ***Treatment*:** The module will send a notification to the department's nodal officer as well as the office of the sub-division of the scheme. The user will receive a unique Grievance ID. ***Ticket closure***: Once the Department has satisfactorily solved the grievance, the ticket will be sent to the resident for closure. If the resident is not satisfied, the ticket can be reopened for further resolution. 2. ***Aadhaar number (Or Aadhaar Reference Key)*** – If the grievance is before the application of the service, the system will raise a grievance and allocate to the owner department of the relevant public service. The grievance can be lodged in self or assisted mode:

S. No.	Requirement Title
	Self-mode: The user will log in to the IPeG portal and navigate to the grievance management module. A grievance ticket can be raised by inputting the Aadhaar number and selecting the grievance from the drop-down menu. The public service for which the grievance is to be raised needs to be selected along with the related department. *Assisted mode*: The user will visit CSC/LSK/CHOiCE or Government Office or call the Call Centre number to lodge a grievance ticket using Aadhaar number. The user informs the executive about the public service for which grievance is to be raised. The executive asks the issue from the resident and selects the relevant option in the dropdown menu. ***Treatment*:** The module will send a notification to the department nodal person as well as the office of the sub-division of the scheme. The executive will provide user with a unique Grievance ID. ***Ticket closure***: Once the Department has satisfactorily solved the grievance, the ticket will be sent to the resident for closure. If the resident is not satisfied, the ticket can be reopened for further resolution. **OFFLINE:** The District Nodal Officer would receive emails or letters from citizens with their grievances. The DGNO will then login using his credentials and lodge a grievance on behalf of the resident. The DGNO will input the details as per the letter and the system will assign the grievance to the relevant departments. In case the grievance is not assigned, the DGNO can assign it manually to a department. In case the DGNO has incomplete information, he can write back to the resident seeking the required data. In that case, the system should be able to lodge a complaint, but put it “pending on resident’s end” status and pause the SLA.
Resolution of grievance	

S. No.	Requirement Title
12.	The grievance can be resolved once the matter is addressed by the relevant authorities. The resolved grievance would be sent back to the resident to get his clearance in closing the ticket.
13.	Once resident gives the approval to close the ticket, the SLA is reset, and the TAT is recorded.
14.	If the resident does not respond to the ticket closure request for more than 30 days, the ticket is automatically closed, and TAT is recorded from the day the ticket was sent to the resident seeking consent for closure of ticket.
15.	In case the resident is not satisfied with the resolution, he/she has the option to keep the ticket open and send it back to the relevant entities.

The MSI shall be responsible to ensure, including but not limited to the following:

- **Solution Design:** The MSI will be responsible to gather the detailed requirement for this toolkit and prepare the detailed design for this component. The design should cover various usage scenarios, ability to configure through simple drag-and-drop, integration with internal and external components for data fetching and data validation, etc.

- **Supply, Installing, Commissioning of IT Software Systems:** MSI is responsible for sourcing, installing and commissioning of the Software Systems for Grievance management on its own cloud infrastructure in PaaS model. It may leverage the same software provided for service delivery application or adopt an open source tool for the same.

- **Software Customization or Integration:** MSI shall be responsible to ensure integration, including but not limited to:
    - Service delivery application toolkit
    - Scheme Analysis, Policy planning and Advanced Analytics toolkit
    - Data related services i.e. Fetch Data, Data Anonymization and Data Identification to obtain the required data
    - Identity authentication and data validation services

- **Software Operations and Maintenance:** The MSI shall be responsible for the maintenance of the tool which includes but not limited to bug fixes, patch upgradation, etc.

- **Provisioning of Licenses:** The MSI will be responsible for providing open source software with enterprise support or they can leverage the licenses for the service delivery application toolkit.

- **Training:** The MSI will be responsible to training to the master trainers of CHiPS. MSI shall be responsible for ensuring all the master trainers are adequately trained to train the end users enabling them to work on the tool. MSI will be required to do (i) Training need assessment, (ii) prepare training plan and content, and (iii) impart trainings and ensure its effectiveness.

- **Handholding support to department:** The MSI shall also be responsible to provide technical support to the departments onboarded on the IPeG platform and using the Grievance management application. The support required to be provided by MSI is as follows:
  - Configuration of forms and attachments required for raising a grievance
  - Configuration of the appellate authorities, resolution workflow for an application. In case of workflow complexities minor coding effort may also have to be undertaken
  - Configuration of notifications or messages that need to be sent to different stakeholders during grievance resolution processing
  - Configuration of output document or payment instructions or any other message that might have to be sent out to the concerned stakeholders
  - Integration with platform services and toolkits under IPeG
  - Configuration of basic reports/ dashboards/ analytics to see how many grievances have been raised, assigned, resolved, overdue etc.

3.2.1.5. Toolkits – Advanced Analytics Tool

The Advanced Analytics Toolkit is envisaged to be a centralized tool which is expected to be used to create actionable information and insights to make public service ecosystem more effective and efficient. The analytics tool will allow business users to generate insights through advanced statistical algorithms on structured / semi structured and unstructured data sets. This will be able to cater to more specialized and higher end needs of the departments, which the scheme analysis and policy planning tool may not be able to address.

Within the Advanced Analytics Toolkit, the departments will be able to apply different criteria to generate insights for decision making. The Advanced Analytics Toolkit will be able to access the data in the social registry through the Data Exchange Gateway. However, the Advanced Analytics Toolkit will not obtain any personal information of the resident, and the data will be shared with the Advanced Analytics Toolkit in an anonymized or deidentified manner. In addition, there should be a facility for the departments to upload their own data for performing analytics on this tool. The requirements are explained in a summarized manner below and for more details, please refer to Annexures.

For the above purpose, CHiPS has planned to provide an Advanced Analytics Tool to the departments of Government of Chhattisgarh. As the departments may not have requisite skills to utilize Advanced Analytics Tool, MSI will deploy its staff who will assist the departments on need basis.

This tool will be used by departments to undertake statistical modelling and rule-based analysis to get detailed insights into how their schemes are being implemented. The analytics tool will allow the user to use statistical models to perform Advanced Analysis/Deep learning, Business Intelligence, Predictive Analysis, trend-analysis, Citizen Grievances Analysis (top reasons, trends, analysed by socio economic, demographic and type etc.) Departments can fetch cross department data in a de-identified form to run statistical models. Effective predictive modelling to accurately determine how successful various citizen services/ schemes are, reducing the overall risk.

Reporting and Analytics Framework of Advanced Analytics Tool should provide a robust set of BI and advanced analytics capabilities enabling different types of users to gain insights from any size of data through data visualization and exploratory analysis. Department users should be able to quickly and easily explore all of your data using a drag-and-drop interface, analyse data and share results easily via Web reports and mobile devices

In addition, the Advance Analytics Tool is expected to be utilized for the following purposes:

- Performance Management & Fraud detection (refer Section 3.2.5.2)
- Scheme analysis & policy planning tool (refer Section 3.2.51.1)
- Data Collection Tool (refer Section 3.2.1.2)

Key requirements are specified below:

- The Creator/Developer/ Analyst users should be able to perform data analytics on both structured and unstructured data
- The Creator/Developer/ Analyst users should be able to prepare data for advanced analytics usage. Data preparation should include (but not limited to) data cleaning, managing data labels, feature engineering, missing value treatment etc
- The user should be able to develop algorithms /models using both supervised and unsupervised analytics techniques. Some of the analytics techniques are as follows:
    - Classifications
    - Regression
    - Clustering
    - Dimensionality reduction
    - Neural networks etc.
- The Creator/Developer/ Analyst users should be able to execute advance analytics algorithms without taking the data out of the system
- The Creator/Developer/ Analyst users should be able to analyse data using OLAP technologies and tools

The MSI shall be responsible to ensure, including but not limited to the following:

- **Solution Design:** The MSI will be responsible to gather the detailed requirement for this toolkit and prepare the detailed design for this component. The design should cover various usage scenarios, integration with internal and external components, etc.

- **Supply, Installing, Commissioning of IT Software Systems:** MSI is responsible for sourcing, installing and commissioning of the Software Systems for Data Collection Tool on its own cloud infrastructure in PaaS model. The proposed solution must have strong advance analytics capability, should be able to integrate with other IPeG components, and should be able to publish analytics results to the departments through an online and an offline mode. The proposed Solution should meet the functional requirement specifications and minimum technical specifications as provided in Annexure.

- **Software Customization or Integration:** MSI shall be responsible to ensure integration, including but not limited to:
    - Data related services i.e. Fetch Data, Data Anonymization and Data Identification to obtain the required data
    - Integration with Common Services Portal, Mobile Application, State DBT Portal, etc. for publication of dashboards

- **Software Operations and Maintenance:** The MSI shall be responsible for the maintenance of the tool which includes but not limited to bug fixes, patch upgradation, etc.

- **Provisioning of Licenses:** The MSI will be responsible for provide unrestricted and perpetual licenses for all data collection exercises to be carried out by the departments. Thus, the license requirements should not be restricted by the number of end-users.

- **Training:** The MSI will be responsible to deployed skilled staff and provide them the training. MSI shall be responsible for ensuring all the staff is adequately skilled to work on the tool.
- **Handholding support to CHiPS and other departments:** The MSI shall also be responsible to provide technical support on the Advanced Analytics Tool. The support required to be provided by MSI is as follows:
    - Configure the use-case scenarios for data analytics for initial requirements which may evolve over time
    - Integration with internal and external data sources for obtaining required data for performing analytics
    - Fine-tuning of analytics scenarios as per evolving requirements of given use-case
    - Publication of insights in business language for consumption of decision making by CHiPS/ department. For non-critical insights, the reports should be generated on a monthly basis. For critical insights requiring immediate attention, the reports should be generated as soon as the insight is detected and brought to the attention of concerned authority in CHiPS/ department.

3.2.2. Platform Services

The MSI shall be responsible to ensure, including but not limited to the following:

- **Solution Design:** The MSI will be responsible to gather the detailed requirement for the platform services and prepare the detailed design for this component. The design should cover various usage scenarios, volume estimation, integration with internal and external

components, creation, and maintenance of microservices, etc. For one platform service, there will be one or more microservices as per specific service being delivered through the concerned platform service.

- **Development, Integration, Installation, Commissioning of Platform Service:** MSI is responsible for development, integration, testing, installation and commissioning of the platform services in a microservices and containerized architecture on its own cloud infrastructure in PaaS model. The proposed database should be an open source solution along with Enterprise support and should be utilized in a PaaS model. The proposed Solution should meet the functional requirement specifications and minimum technical specifications as provided in Annexure. MSI shall publish the platform service on a common IPeG platform. MSI shall be responsible to ensure integration, including but not limited to:
  - External sources of electronic government identity (e.g. Driver's License, PAN Card, etc.)
  - All components of IPeG solution provided by MSI

- **Software Operations and Maintenance:** The MSI shall be responsible for the maintenance of the service which includes but not limited to bug fixes, patch upgradation, performance optimization, etc. The MSI should aim to utilize the latest version, or previous versions (in case of stability issues in latest version) of software. In case, the MSI requires exemption from this, the MSI should request the CHiPS for such an exemption giving clear reasons for this request.

- **Provisioning of Licenses:** The MSI will be responsible to provide licenses, as necessary. Thus, the licenses should be sufficient to meet the scaling requirements.

- **Training and Documentation:** The MSI will be responsible to undertake the requisite training for operation, maintenance, handholding, etc. The functional support and coordination will be carried out by the CHiPS in-house team and MSI will be required to provide them necessary trainings and documentation.

- **Technical Support:** The MSI will be required to provide technical services as described below:
  - Prepare, update and maintain the documentation.
  - As part of technical services, provide technical support to the concerned departments (Section **Error! Reference source not found.**) which are interested in utilizing the p latform service and are utilizing the platform service.
  - Monitor the usage and health and provide necessary report(s) and recommendations to CHiPS (on usage and health)

- **Functional Support (CHiPS In-house Staff)**: The CHiPS in-house staff will carry out the following:
  - coordinate with interested departments to describe the associated platform services, assist in onboarding, monitoring utilization, etc.

- enable, disable, suspend or resume platform services for specific department(s), user(s) and user-group(s), etc.

3.2.2.1. Platform Service – Identity Authentication Service

For delivering the public services, the government departments may be required to authenticate the citizens and/or obtain their demographic details. Identity Authentication platform service would help facilitate identity authentication in both Aadhaar and non-Aadhaar scenarios. For the Identity Authentication platform service multiple microservices may have to be built and MSI should design the same accordingly. On the basis their business requirements, departments can avail one or more of the services of identity authentication. The usage scenarios are described below:

A. Aadhaar based identity authentication

UIDAI extends broadly following kinds of Aadhaar authentication/verification services:

- Identity Authentication using Aadhaar (known as “Aadhaar Authentication”) by which the Aadhaar number along with the demographic information or biometric information of an Aadhaar number holder or an OTP is submitted to the UIDAI for its verification on the basis of the information available with it and it returns a Yes/No response.
- Obtain demographic details as in Aadhaar (known as “e-KYC”)
- Offline verification method using Aadhaar Paperless Offline e-KYC, and Aadhaar validation using QR Code reader

For delivering the first two services, CHiPS is a AUA/KUA and the departments of the GoCG will be able to utilize identity authentication using Aadhaar Authentication and Aadhaar e-KYC platform services through CHiPS. While AUA/KUA set up is outside the scope of this project, the service that departments will utilize to connect with the AUA/KUA service will have to be developed by the MSI.

B. Non-Aadhaar based identity authentication

For Non-Aadhaar based identity authentication, there would be 3 possible scenarios:

- **Digital Authentication using Aadhaar linked Government IDs** – Government IDs which have been onboarded onto IPeG and linked to Aadhaar number (Aadhaar Vault ID) can be used to digitally authenticate identity. MSI need to develop solution so that, this would be carried out by first finding out the Aadhaar Vault ID (mapped to the Government ID) of the citizen, then fetching Aadhar number from Aadhaar Data Vault and then utilizing the Aadhaar authentication mechanism.
- **Other accepted electronically verifiable government ID** – In this case, the accepted government ID would be verified by the issuing authority’s records.
- **Other accepted electronically unverifiable government ID** – In this case, the concerned individual would visit an authorized service centre/Government office where government official/authorized personnel would validate the identity of individual using the physical copy

of the concerned government identity (e.g. PAN Card, Voter Card, MGNREGA Job Card, etc.).

For more details on this platform service, please refer to the Annexures.

3.2.2.2. Platform Service – Aadhaar Vaulting Service

CHiPS will provide this component and role of the MSI will be limited to integration with Aadhaar vault service and its utilization in this solution.

3.2.2.3. Platform Service – SRN Vault

A 'Social Registry Number' (SRN) will be created using SRN vault service and will be mapped to this 'Aadhaar Vault ID (Reference Number).The IPeG Platform will provide an additional identity referred to as Social Registry Number (or SRN). The departments need to store the SRN in their beneficiary database along with Aadhaar Reference Key. Using this SRN, the IPeG will facilitate secure information exchange, through a pre-defined data exchange rules and protocols including privacy controls as defined in the Data Exchange Guidelines and Framework notified by CHiPS.

3.2.2.4. Platform Service – Seeding Validation Service

For direct benefit transfer, there is a need to undertake the seeding in the department databases. The seeding may comprise of inclusion of correct Aadhaar number, bank account details, etc. To ensure the correctness of information being seeded, it is important to ensure the validation is performed on corresponding details. This platform service will be used for the purpose of performing such validations and may comprise of multiple microservices, as necessary. For more details on this platform service, please refer to the Annexures.

Once Aadhaar (or other details) are seeded in department database, there might be multiple levels of validation a department might need to perform. The seeding validation platform service will cater to all these requirements of a department, ensuring accurate seeding in department database:

- Whether the Aadhaar number itself is a valid or correct number (Verhoeff algorithm check)
- Whether the Aadhaar number is seeded against the right beneficiary information (Aadhaar Authentication)
- Whether the Aadhaar number is linked to a bank account to initiate Aadhaar based payments (lookup on NPCI mapper)
- Whether the IFSC code is correct and corresponds to a bank branch in state. For list of IFSC codes, the MSI will need to maintain a database using the details available on website of Reserve Bank of India (https://www.rbi.org.in/scripts/neft.aspx).

In addition to the platform service, the MSI will be required to provide and maintain the Verhoeff algorithm code which can be integrated by department in their web-based and mobile-based applications (for offline use) independent on the software development languages (Java, .Net, PHP, Android, iOS, etc.). The software code should be available to enable plug-and-play usage with minor customization in department applications for which the MSI may provide necessary standardized integration documentation to the departments.

3.2.2.5. Platform Service – Payment Disbursal Service

As per the mandate of Direct Benefit Transfer (DBT), the social benefits need to be transferred to beneficiary's bank account using PFMS. At present, there are multiple DBT schemes in the state (CSS & SS) which are presently not paying through PFMS.

PFMS being a system of the Government of India intends to integrate with a limited set of systems from every state i.e. it does not intend to integrate separately with all the different department systems used by various schemes. In view of this, it is envisaged to offer a solution to all departments a standard service of 'Benefit disbursal through PFMS' for their DBT schemes. This service would act like a bridge between different scheme systems and the PFMS system. For more details on this platform service, please refer to the Annexures.

This service will be integrated in the department systems as well as Service Delivery Application Toolkit and Grievance Toolkit. The MSI will be required to design, develop and implement the service to cater to all the requirements of payment disbursal and reconciliation through PFMS. After the rollout of this service, the MSI will be required to provide necessary integration documentation and technical support.

The overview of the solution requirements of the 'Platform for payment through PFMS' has been outlined below:

- It should be able to consume data through APIs from different existing/upcoming systems (beneficiary management) of different schemes
- It should be able to generate XML files in the format as required by PFMS
- It should support digital signature capabilities and enable digital signature on XML files generated by concerned government officials
- It should be able to push XML files to SFTP server of PFMS
- It should be able to pull reconciliation or response files from the SFTP server of PFMS
- It should be able to send mobile message and email notifications to the registered department users.
- It should be able to generate dashboard or MIS reports
- It should be unable to perform all payment methods supported through PFMS.
- This system should enable to generate error file received form PFMS system
- This system should capable of sending payment advice to the bank automated way using digital signature.

In addition to the above, the MSI will be required to provide technical services as described below:

- Integration support to the department for availing PFMS based service delivery using this application.
- Prepare a presentation which can be used by CHiPS in-house team. For this purpose, MSI can refer to PFMS user manual issued by CGA for onboarding schemes in PFMS platform.
- Develop user manual for operating the new solution which is integrated with PFMS.

The in-house staff of the CHiPS will perform below mentioned activities:

- Facilitating the departments to understand end-to-end PFMS onboarding process starting from Program division registration – Child agency creation – Creation of Users (Maker and Checker)- fund disbursal to end beneficiary.

3.2.2.6. Platform Service – Payment Receipt Service

In multiple public services, the citizens are required to make payment of fees for availing the service. At present, some of the department systems have integrated with payment gateway for enabling online receipt and reconciliation of such fees. However, some department systems may still require enablement of online receipt and settlement/reconciliation of fees. This platform service will enable the aforementioned purpose. For more details on this platform service, please refer to the Annexures.

The MSI will be required to develop a payment service in a manner of integration with payment gateway (e.g. PayGov). This service will help government departments in acceptance of all payment modes/options (UPI, credit card, debit card, online banking, NEFT/RTGS, wallets, etc.) permitted by Reserve Bank of India, and Department of Finance, Government of Chhattisgarh.

This service will be integrated in the department systems as well as Service Delivery Application Toolkit and Grievance Toolkit. The MSI will be required to design, develop and implement the service to cater to all the requirements of payment receipt and settlement/reconciliation. After the rollout of this service, the MSI will be required to provide necessary integration documentation and technical support. This application should have following features-

- One solution for receiving all payments, which department can integrate easily to their service delivery application.
- should be capable of generating MIS as per the requirement and format prescribed by the government
- this application should provide lookup facility for transaction status, settlement/reconciliation status, refund request status, etc.
- The user should be clear shown the applicable fees and success ratio of each of the payment modes/options so that they can opt for a suitable option
- this service should be a single point technical integration for the departments i.e. there for departments there should not be a need to integrate with multiple bank(s) or payment gateway(s).

To begin with, the MSI will be required to integrate with payment gateway prescribed by Government of India i.e. PayGov. However, on a later date the CHiPS may onboard payment gateway(s) and MSI will be required to integrate with them.

CHiPS will enter into direct agreement with the payment gateway provider(s) and will bear the costs associated to security deposit, agreement, etc. The recurring costs related to service charges levied by payment gateway provider(s) may either be borne by respective department(s)/CHiPS or may be passed onto the citizens. The MSI will be responsible for assisting CHiPS in negotiation, signing agreements, and coordination with payment gateway provider(s).

In addition to the above, the MSI will be required to provide technical services as described below:

- Integration support to the department for availing this service

- Prepare a presentation which can be used by CHiPS in-house team to inform the department about this service
- Develop user manual for operating the new solution
- Monitor the performance and provide suggestions for areas of improvements
- Perform operational activities related to settlement, reconciliation and refund (including loading of scrolls/reports received from banks, enlistment of complaints for refund, etc.)

The in-house staff of the CHiPS will perform below mentioned activities:

- Enlistment of service for the given payment gateway provider(s)
- Coordination with the payment gateway provider(s) for their onboarding
- Perform decision-making activities related to settlement, reconciliation and refund

3.2.2.7. Platform Service – Fetch Data Service

The data about the citizens will be stored in respective data sources(s). However, one of the data source(s) will be designated as a master or owner of a particular data field. This platform service will be used to fetch data from respective data source(s) i.e. registries as well as other public service databases onboarded onto IPeG. One of the main usages of this service will be used to auto-populate the scheme application forms. Another usage of this service will be to validate/verify of these data received in application forms by the government officials. The microservices created for fetch data (a request may be sent to concerned data source and the data values may be received as response) should be separate from ones created for data validation (for verification the data may be sent to concerned data source and a 'Yes/No' response may be received).

This service will be integrated in the department systems as well as Service Delivery Application Toolkit, Grievance Toolkit, other toolkits and Data Exchange Gateway. The MSI will be required to design, develop and implement the service to cater to all the requirements. After the rollout of this service, the MSI will be required to provide necessary integration documentation and technical support.

This service should have following features:

- Enable data fetch and data validations using Reference Key as well as SRN ID
- Ensuring encryption and decryption processes during fetch data services
- Integration with Data Exchange Gateway as an enabling system for this service

In addition to the above, the MSI will be required to provide technical services as described below:

- integration with Data Exchange Gateway as an enabling system (Section 3.2.5.5)
- technical support to the department for availing this service

The in-house staff of the CHiPS will perform below mentioned activities:

- define the master data source for each data field
- coordinate on administrative and functional aspects with concerned department i.e. master data source

3.2.2.8. Platform Service – Push Data Service

The data about the citizens will be stored in respective data sources(s). However, one of the data source(s) will be designated as a master or owner of a particular data field. When the citizen's data gets updated in the master/owner data source, this service will be used to inform all the subscribed system(s) about the update in the information. The data will be pushed or published to only those concerned database or registries which have subscribed to receiving such updates. For this purpose, the concerned system(s) will be required to register/subscribe as a consumer for this service and concerned data field(s) which are relevant to them.

This service will be integrated in the department systems as well as Service Delivery Application Toolkit, Grievance Toolkit, and Data Exchange Gateway. The MSI will be required to design, develop and implement the service to cater to all the requirements. After the rollout of this service, the MSI will be required to provide necessary integration documentation and technical support.

This service should have following features:

- enabling data push services using Reference Key as well as SRN ID.
- ensuring encryption and decryption processes during push data services
- should have feature to publish the updated/new beneficiary details among participants departments
- developing business rule for enabling push data services so that specific data attribute will be published to specific departments.

In addition to the above, the MSI will be required to provide technical services as described below:

- integration with Data Exchange Gateway as an enabling system (Section 3.2.5.5)
- technical support to the department for availing this service

The in-house staff of the CHiPS will perform below mentioned activities:

- define the master data source for each data field
- coordinate on administrative and functional aspects with concerned department i.e. master data source

3.2.2.9. Platform Service – Publish Document Service

The departments or the citizen themselves can store marksheets and certificates to the digital locker. This service may be used by the departments to publish their documents to the digital locker with due consent from the citizen.

This service will be integrated in the department systems as well as Service Delivery Application Toolkit, Grievance Toolkit, and Data Exchange Gateway. The MSI will be required to design, develop and implement the service to cater to all the requirements. After the rollout of this service, the MSI will be required to provide necessary integration documentation and technical support.

In addition to the above, the MSI will be required to provide technical services as described below:

- integration with Data Exchange Gateway as an enabling system (Section 3.2.5.5)
- integration with Digital Locker of the Government of India
- integration with consent repository of IPeG
- technical support to the department for availing this service

The in-house staff of the CHiPS will perform below mentioned activities:

- finalize the MoU or necessary documentation with Digital Locker
- coordinate with document issuing authorities (provider departments) and assist them to register on Digital Locker as the issuer(s)
- coordinate with document receiving authorities (consumer departments) and assist them to register on Digital Locker as the requester(s) or verifier(s) enabling them to verify the documents with consent from citizens

3.2.2.10. Platform Service – Anonymization and Deidentification Service

To ensure the privacy of citizens data, there will be a need to anonymize the citizen's data. Through anonymized data it is not feasible to identify the individual to whom the data corresponds to. As per the Personal Data Protection Bill, the "anonymisation" in relation to personal data, means *such irreversible process of transforming or converting personal data to a form in which a data principal cannot be identified, which meets the standards of irreversibility specified by the Data Protection Authority of India established under the provisions of the Bill;*

To ensure the privacy of citizens data, there will be a need to de-identify the citizen's data. Through de-identified data it is feasible to re-identify the individual to whom the data corresponds to. As per the Personal Data Protection Bill, the " de-identification" in relation to personal data, means *the process by which a data fiduciary or data processor may remove, or mask identifiers from personal data, or replace them with such other fictitious name or code that is unique to an individual but does not, on its own, directly identify the data principal;*

The MSI will be responsible to:

- Study the various data elements which are part of the Social Registry within IPeG and propose the categorization of various the data elements (personal or non-personal, etc.)
- Study the relevant standards, including but not limited to the following:
    - **ISO 27000:** Information technology — Security techniques — Information security management systems — Overview and vocabulary
    - **ISO 20889:** Privacy enhancing data de-identification terminology and classification of technique
    - **ISO/IEC 29100:** Information technology — Security techniques — Privacy framework
- Study the leading data privacy standards, models, and techniques
- Study the legal framework around data security and data privacy in India, including but not limited to the following:
    - Personal Data Protection Bill (as amended or enacted from time-to-time) including regulations, rules, circulars, orders, etc.
    - Information Technology Act (as amended from time-to-time) including regulations, rules, circulars, orders, etc.

- Prepare the anonymization and de-identification protocol for various data elements being stored or exchanged under the IPeG program, in consultation with CHiPS
- Configure, Manage and Monitor the approved anonymization and de-identification protocol(s) on the IPeG components i.e. Social Registry, Data Exchange Framework, etc.

3.2.2.11. Platform Service – Telemetry Service

The user experience and behaviour forms the core of usability of the IT solutions. As part of IPeG, the solution components needs to be intuitive, user-friendly, and convenient for end-users. For analysing the user behaviour and improving the user experience, there will be a need to generate rich insights on the manner in which the users use the IT components of IPeG.

The IPeG platform shall be capable of capturing the trail of every click of the users (prospective beneficiaries, platform admins, scheme owner users, any other users of the platform) and record into the database. This will help in understanding the areas of improvements and personalization. In addition, the telemetry information may be useful to monitor the application health, quality, and performance.

The collection and analysis of such information will be done in a standardized manner which will be useful for existing IT applications as well as new applications. Thus, telemetry will be provided as a platform service.

Telemetry service will generate large amount of data which may become obsolete and outdated after some time. Thus, on a periodical basis the data will be archived and purged. For this purpose, the MSI will be required to propose the data archival and purging policy in consultation with CHiPS. Once the policy is approved, the MSI will be required to configure the same in the telemetry component on the product environment.

3.2.2.12. Platform Service – Feedback Service

The standard form of citizen feedback and satisfaction will be available for usage as a service. The feedback will be collected for each interaction of the citizen with the government for public service delivery. In addition, additional parameters may be identified for which feedback or satisfaction may be sought from the citizen. Using this feedback and satisfaction response, the government will be able to identify the areas for improvement.

The feedback may be initiated through the omnichannel interface. While initiating the feedback, the user-preference may be considered. For example, senior citizens may choose their preferred medium as IVR based call, the students may choose social media (e.g. WhatsApp) as their preferred medium.

The feedback may be initiated in push-mode as well as pull-mode. In push-mode, the government may seek the feedback from the concerned resident, and this can be done as per user preference or other settings as defined for concerned scenario. In pull-mode, the resident may provide the feedback for any public service interaction. The feedback service may be utilized for the simple feedback (e.g. 5-star, 10-point rating scale, etc.).

The feedback services should be able to handle feedback requests and responses. In addition, the feedback service should be analysed by the MSI for developing insights and recommendations on the areas of improvement. For generation of insights, the platform service may utilize other components of platform i.e. Scheme Analysis and Policy Planning Tool and/or Advanced Analytics Tool. The MSI will also be responsible for required integration with aforementioned components, analysis and insight generation.

This service will be integrated in the department systems as well as Service Delivery Application Toolkit and Grievance Toolkit. The MSI will be required to design, develop and implement the service to cater to all the requirements. After the rollout of this service, the MSI will be required to provide necessary integration documentation and technical support.

In addition to the above, the MSI will be required to provide technical services as described below:

- integration with Messaging Service to send request and receive response for feedback
- integration with Advanced Analytics Toolkit for generation of insights, rankings/ratings, etc.
- integration with Policy Planning Toolkit for generation of reports and dashboards
- integration with Access Channels receiving feedback and showing the reports/dashboards

The in-house staff of the CHiPS will perform below mentioned activities:

- coordinate with department having their own IT systems for service delivery
- monitoring and reporting to concerned stakeholders, including potential actionable

3.2.2.13. Platform Service – Schedule Appointment Service

This service application will be used by the citizen, to schedule appointments on basis of business requirements (e.g. re-submission of documents based on remarks provided by approving authority, etc.) for service delivery outlets or government office. MSI need to develop the microservice for scheduling of appointment. The indicative services for enablement of this platform service is as follows:

- Scheduling the appointment for an individual or family, cancel appointment, reschedule appointment, etc.
- Analytics to identify cases of suspected booking(s) by middleman, etc. and incorporation of preventive measures such as limited appoints for a given identity, etc.

The resident should have allowed to provide below mentioned inputs during scheduling an appointment:

- **Application number** in relation to which the appointment is sought (optional)
- **Requester Details** like Name, Father Name, Contact details, Reason for appointment etc.
- **Time:** Date and Time of appointment
- **Location:** Service Delivery Centre, or Government Office
- **Request Type:** appointment booking, rescheduling or cancellation
- **Appointment details** – reference Number (if any) for rescheduling or cancellation cases

In addition to the above, the MSI will be required to provide technical services as described below:

- integration with Messaging Service to sending communication related to appointments
- integration with Advanced Analytics Toolkit for generation of insights, rankings/ratings, etc.
- integration with Policy Planning Toolkit for generation of reports and dashboards
- integration with Access Channels appointment related interactions

The in-house staff of the CHiPS will perform below mentioned activities:

- coordinate with department having their own IT systems for service delivery
- monitoring and reporting to concerned stakeholders, including potential actionable such as change in time-slot per application, cases of complaints for not honouring appointments/other malpractices, etc.

3.2.2.14. Platform Service – Translation Service

To make the public services more convenient to the residents, it is important to communicate with them in their language of choice. In addition, to make the service delivery more efficient, it may be important to display information to government officials in their preferred language. Additionally, data entry happens in local language for some schemes, however, to ensure compatibility with different state government and central government systems, it is important to have all data in English to ensure interoperability.

The interaction will span across various access channels such as web portal, mobile application, call centre, etc. which will have multi-lingual interface. In addition, the interaction will be with multiple applications such as Service Delivery Application, Grievance Management, etc. which are also multi-lingual in nature.

The translation and transliteration services will be used by the IPeG components as well as the existing IT solutions of the department. Hence, it has been categorized as a platform service with standard input and output format. The consumer applications will access this service to translation/transliterate the content from English to local language (or vice-versa). This service should accept the input as various data format (ASCII[4], ISCII[5], UNICODE, etc.) in one-language and output as UNICODE in another language.

The IPeG platform shall have language translation and transliteration components to convert the English language to the local language and vice versa. The translation and transliteration services may useful for the following:

- Display of application forms and interfaces to the end-user in local language using transliteration feature
- In most cases, the end-user may enter in English language. However, in case entry is done in local language across the solution components, it needs to be translated to English language using translation service.
- In the future, speech to text conversion (and vice versa) and text to text language translation capabilities shall be widely used.

[4] ASCII refers to American Standard Code for Information Interchange
[5] ISCII refers to Indian Script Code for Information Interchange

The MSI will be required to supply the underlying translation and transliteration software and utilize the same to develop the platform service. The bidder should evaluate the solution provided by the government i.e. CDAC as well as other solutions and propose the translation/transliteration tool in a manner wherein the quality of output is as per the expectations of a common resident. In case, the proposed solution does not provide satisfactory quality of output, CHiPS may ask the bidder to replace the proposed solution with better quality solution free-of-cost to CHiPS.

In addition to the above, the MSI will be required to provide technical services as described below:

- integration with Messaging Service to translation of outward or inward communication

The in-house staff of the CHiPS will perform below mentioned activities:

- coordinate with department having their own IT systems for service delivery
- sign necessary agreement/MoU with CDAC, in case it is proposed by the bidder
- coordination with CDAC, for submission of suggestions related to quality improvements

3.2.2.15. Platform Service – Messaging Service

This will be a centralized application which can be accessed by all departments on IPeG to send messages and notifications to relevant stakeholders. The messaging service should be able to send messages through SMS, Email, Social Media (WhatsApp, Facebook, etc.). The features required in this service are as follows:

- Application should have provision of push and pull messages for outward and inward communication respectively
- Application should have provision of push messages to individuals as well as groups
- The mode of message service should be through multiple channels such as SMS, e-Mail, Social Media (WhatsApp, Facebook, etc.), etc.
- The system should have capable to provide pre-recorded information messages to callers through integration with call centre application (only outward communication)

CHiPS will provide the SMS gateway as well as Email gateway and will also bear the associated transaction charges. Similarly, CHiPS will bear the associated transaction charges for social media transactions (WhatsApp, Facebook, etc.).

In addition to the above, the MSI will be required to provide technical services as described below:

- integration of Messaging Service with all relevant components of IPeG
- monitor uptime of associated components (e.g. SMS Gateway, Email Gateway, etc.) and raise tickets for corrective actions

The in-house staff of the CHiPS will perform below mentioned activities:

- coordinate with SDC team for email gateway related issue
- coordinate for signing necessary agreement/MoU with Social Media organizations, in case it is proposed by the bidder

3.2.2.16. Platform Service – Single Sign-On Service

In order to ensure that citizen or the government authorities do not need to login multiple times to avail different applications or services, single sign-on feature would be integrated with the common service portal and the mobile app for both government authorities and citizen. For this service, the Single Sign-On will be an enabling component. The SSO solution shall bring following advantages to departments & users:

- It may enable users to login with single passwords and usernames for each application.
- It may streamline the process of signing on and using applications - no need to remember multiple passwords.
- It may lead to fewer complaints or tickets about passwords in helpdesk.

Enabling system for SSO

This component would work as an enabling component for 'Platform Service – Single Sign-On'. This solution should have following feature:

- The product must support Open Standards like SAML 2, o-Auth 2, OpenID Connect, WS-Security and WS Federation
- The product must support Implementation of SAML 2 Identity Provider and SAML 2 Service Provider for authentications based on SAML2
- The solution should support global idle session timeout, session timeout for idle sessions and single log-out
- SSO to Cloud applications: Must support SSO with applications hosted on cloud
- Support for SSO to legacy applications
- Should integrate with SIEM
- Support for SSO using reverse proxy
- The bidder should configure SSO between landing page and backend system/application on different platforms like java, .net, php etc.
- The SSO solution should have following advantages:
    - It should enable users to login with single passwords and usernames for each application.
    - It should streamline the process of signing on and using applications - no need to renter passwords.
    - It should lessen the chance of phishing.
    - It should lead to fewer complaints or trouble about passwords for IT help desks.

The MSI should consider utilizing the Single Sign-On (SSO) solution of Government of India developed by NIC, or any other solution deemed suitable for this component

3.2.3. Data Sources (Social Registry)

The MSI shall be responsible to ensure, including but not limited to the following:

- **Solution Design:** The MSI will be responsible to gather the detailed requirement for the platform services and prepare the detailed design for this component. The design should cover various usage scenarios, volume estimation, integration with internal and external components, creation, and maintenance of data sources, etc.

- **Development, Integration, Installation, Commissioning:** MSI is responsible for development, integration, testing, installation and commissioning of the data sources on its own cloud infrastructure in PaaS model. The proposed database should be an open source solution along with Enterprise support and should be utilized in a PaaS model. The proposed solution should meet the functional requirement specifications and minimum technical specifications as provided in Annexure. MSI shall be responsible to ensure integration, including but not limited to all relevant components of IPeG solution provided by MSI

- **Software Operations and Maintenance:** The MSI shall be responsible for the maintenance of the service which includes but not limited to bug fixes, patch upgradation, performance optimization, etc. The MSI should aim to utilize the latest version, or previous versions (in case of stability issues in latest version) of software. In case, the MSI requires exemption from this, the MSI should request the CHiPS for such an exemption giving clear reasons for this request.

- **Provisioning of Licenses:** The MSI will be responsible to provide licenses, as necessary. Thus, the licenses should be sufficient to meet the scaling requirements.

- **Training and Documentation:** The MSI will be responsible to deployed skilled technical staff as part of the technical helpdesk and provide them the requisite training for operation, maintenance, handholding, etc. The functional support and coordination will be carried out by the CHiPS in-house team and MSI will be required to provide them necessary trainings and documentation.

- **Technical Support:** The MSI will be required to provide technical services as described below:
  - Prepare, update and maintain the documentation.
  - As part of technical services, provide technical support to the concerned departments (Section **Error! Reference source not found.**) which are interested in utilizing the data s ource(s) and are utilizing the data source(s).
  - Monitor the usage and health and provide necessary report(s) and recommendations to CHiPS (on usage and health)

- **Functional Support (CHiPS In-house Staff)**: The CHiPS in-house staff will carry out the following:
  - coordinate with interested departments to describe the associated data source(s), assist in onboarding, monitoring utilization, etc.
  - enable, disable, suspend or resume data source(s) for specific department(s), user(s) and user-group(s), etc.

3.2.3.1. Data Sources – Social Registry

The registries are trusted sources of data elements (information and documents) of residents' i.e. individuals whose native state is Chhattisgarh and people living in Chhattisgarh state, which are required for the purpose of public service delivery to the citizens. The residents' data would be

stored across different federated social registries that can exchange data with each other through the Data Exchange Gateway to enable efficient/proactive service delivery. The exchange of data will be as per the Data Exchange Framework Guidelines of IPeG program.

The Social Registries containing citizen data would broadly be of following two types:

- **Federated Social Registry (Centralized):** This would centrally store some commonly used resident data at one place viz. Name, Date of birth, Gender, Address, Ration card number, Aadhaar Vault ID (Reference number) etc. The exact set of data fields will be provided by CHiPS during the requirement gathering phase of the MSI. A minimalistic approach will be adopted for creation of this centralize federated social registry i.e. only those data elements will be stored centrally which are essential for public service delivery and not owned by any specific department. The remaining data elements will be stored by the departments in its department databases (e.g. BPL/APL status in PDS, etc.) and in their Decentralized registries

- **Federated Social Registries (Decentralized):** These registries would store information about residents specific to particulars schemes/service. This will be hosted by concerned departments which are owners of respective information.

1. **Creation of a Centralized Federated Social Registry and a 'SRN ID'**
    a. A large beneficiary database with higher percentage of Aadhaar Seeding (e.g. PDS database) would be used as a base for creation of Centralized Federated Social Registry.
    b. This large beneficiary database would share Aadhaar Numbers for Aadhaar Vaulting. At the time of undertaking Aadhaar Vaulting, a demographic authentication of records would be undertaken to ascertain if Aadhaar Seeding is accurate.
        1) For records with accurate Aadhaar Seeding
            i) Aadhaar Numbers would be stored in Aadhaar Data Vault and an Aadhaar Vault ID (Reference Number) would be generated.
            ii) A 'SRN ID' *(Aadhaar Vault ID (Reference Number) or a 'Social Registry Number (SRN)' mapped to this 'Aadhaar Vault ID (Reference Number))* shall be created and shared with the concerned department for them to store in their database (Registry) in place of Aadhaar Numbers.
            iii) This 'SRN ID' and the corresponding 'Aadhaar Vault ID (Reference Number)' shall also be stored in a separate database/registry maintained by CHiPS which shall called 'Centralized Federated Social Registry'
        2) For records with inaccurate Aadhaar Seeding
            i) Concerned department would be asked to correct the Aadhaar Seeding
            ii) Correctness of Aadhaar Seeding would be checked again as per the process described above
            iii) For records with accurate Aadhaar Seeding, above mentioned steps under 'For records with accurate Aadhaar Seeding' would be undertaken
    c. Over a period of time, different department registries, as and when they vault Aadhaar Numbers in their database, would be used to add resident records in 'Centralized Federated Social Registry'. The objective would be, to add records of residents with accurate Aadhaar Seeding in department databases over a period of time to the 'Centralized Federated Social Registry' and seed 'SRN ID' in as many department beneficiary databases as possible.

d. The Centralized Federated Social Registry will have following fields:
   i) **SRN ID** of all residents for whom some department of Govt. of Chhattisgarh has undertaken an accurate Aadhaar Seeding and have then vaulted the Aadhaar with 'Aadhaar Data Vault' under IPeG program.
   ii) **Aadhaar Vault ID -** If 'SRN ID' is designed to be different from 'Aadhaar Vault ID (Reference Number)' then Centralized Social Registry shall have 'Aadhaar Vault ID (Reference Number)
   iii) Other fields such as name, gender, date of birth etc. The exact fields to kept would be finalized during the roll-out phase after detailed study of requirements of common fields and need to store in the Centralized Social Registry. However, the number of fields will be kept to a minimum number.

2. Seeding of 'SRN ID' in Decentralized Federated Social Registries

a. The 'SRN ID' would be seeded in all registries containing citizen data over a period time as they vault the Aadhaar numbers present with them.
b. Departments, when they avail 'Aadhaar Vaulting' service offered under IPeG, would share Aadhaar Number to be stored in 'Aadhaar Data Vault' and in return would get Aadhaar Vault ID (Reference Number) or a 'SRN ID' (e.g. Social Registry Number) mapped to this Aadhaar Vault ID (Reference Number).
c. Over a period of time, commonly used identities as Ration Card shall also be seeded with this 'SRN ID'. These identity databases would first need to seed Aadhaar and then vault their Aadhaar with 'Aadhaar Data Vault' under IPeG program. They would then in return get the 'SRN ID' which they shall seed in their databases.
d. All departments with beneficiary database would be encouraged to seed this 'SRN ID' to the extent possible

3. Use of 'SRN ID' for exchange of data

This 'SRN ID' would be used to exchange citizen data between different registries/departments through IPeG Data Exchange Platform. For example, when a resident applies for a services onboarded onto IPeG, using Aadhaar Number or any other ID mapped to the 'SRN ID', the 'SRN ID' shall be used to fetch his/her data available with different departments, where this 'SRN ID' has already been seeded. This would enable auto-population of data/information/documents, helping reduce resident inconvenience of providing same data/information/documents multiple times and it would also help system assisted authentication of data/information/documents by Government officers since data/information/documents are fetched from a reliable data source.

The MSI is expected to ready the database schema, create APIs which can be accessed through the data exchange platform of IPeG for creating, updating, reading or passivizing entries into this database.

Note: Merging of registries and obtaining standardized reports are functionalities that will have to be built by the MSI for Social registry as well as other registries

The scope of work can be divided into 4 major pillars:

Step	Description
Creation	• The MSI is expected to coordinate with CHiPS and other line departments to create the robust database pertaining to Federated Social Registry (centralized) and corresponding APIs, to be used by departments onboarding to IPeG, through the data exchange platform. The tentative list of data fields to be kept centralized have been provided in Annexure - IV. These fields will be re-examined during the requirement gathering phase by the MSI. • The MSI is expected to coordinate with CHiPS and line departments of 5 shortlisted public services to create the robust database and corresponding APIs for usage by other departments onboarding to data exchange platform of IPeG. The details of 5 public services have been provided in Annexure–V. • These decentralized fields will keep expanding as more and more state public services are onboarded to IPeG. Therefore, it is expected that the MSI in coordination with IPeG PMU would establish standard operating procedures for departments to contribute to the Social registry. • Train all the interested line departments in technology and process for onboarding to Social registry and creating of APIs for data exchange.
Read/View	• The MSI is expected to coordinate with CHiPS and other line departments to create robust technology and process mechanisms through which data fields can be read in the centralized fields of the Social registry. The user access controls and different levels of permission to read a particular data filed will be finalized during the requirement gathering phase by MSI. • The MSI is expected to coordinate with CHiPS and line departments of 5 shortlisted public services to create robust technology and process mechanisms through which data fields can be read. The user access controls and different levels of permission to read a particular data filed will be finalized during the requirement gathering phase by MSI. • With increase in the number of public services onboarded on IPeG, the decentralized fields will keep on increasing. This implicates a greater number of fields that need to be read. The MSI should develop a standard set of APIs which can be invoked to read the requisite data by a concerned stakeholder department. The details would be defined in an SOP, which would be developed and is part of the scope of work under Social registry creation, as mentioned above.
Update	• The MSI is expected to coordinate with CHiPS and other line departments to create robust technology and process mechanisms through which data fields can be updated in the centralized fields of the Social registry. The

Step	Description
	user access controls and different levels of permission to update a particular data filed will be finalized during the requirement gathering phase by MSI. • The MSI is expected to coordinate with CHiPS and line departments of 5 shortlisted public services to create robust technology and process mechanisms through which data fields can be updated. This involves creation of triggers and APIs with data field owner departments. For example, a public service implementation requires caste, income data and the same is part of the decentralized fields. In this scenario, owner department of caste and income data is revenue department. In case there is any change with respect to these data fields in the revenue department then the same change must reflect in the decentralized fields of the Social registry. The user access controls and different levels of permission to update a particular decentralized data filed will be finalized during the requirement gathering phase by MSI. • With increase in the number of public services onboarded on IPeG, the decentralized fields will keep on increasing. This implicates a greater number of fields that need to be kept updated. The MSI should develop a standard set of APIs and triggers which can easily be configured by data field owner departments, as and when they come onboard. • MSI also needs to provide requisite training to the departments nominated by CHiPS, so that they can easily consume and configure APIs on need basis.
Passivate / Activate	• MSI is expected to coordinate with CHiPS and other line departments to create standard operating procedures and configuration changes to passivize any centralized data field in social registry. The user access control for this functionality should lie entirely with CHiPS • MSI is expected to coordinate with CHiPS and line departments of 5 shortlisted public services to passivize any decentralized data field. The user access controls, and necessary permissions would lie with the data field owner department but would also need prior approvals from the concerned public service implementing department and CHiPS. This will again be part of the SOP to be drafted in consensus between the line departments, CHiPS, PMU team and the MSI. • MSI will train all the interested line departments who onboard on IPeG, with regard to processes and technology changes that need to be made for passivation of data fields.

3.2.3.2. Data Sources – Index of Registries

Over a period of time, as the program gets rolled out, there will be various registries which will be setup to meet the requirements of IPeG program. An index of registries shall also be created, that shall contain list of all the registries under IPeG program, and brief details about them.

The entire lifecycle of this component has four types of interactions i.e. creation, update, view and passivation. The MSI will be responsible to design, development, install, operation and maintain the registry. As part of the design, the MSI will be responsible to define data fields, permissible interactions and conditions, interaction mechanisms (APIs), access controls and authorization mechanisms, relationships (parent-child, siblings, etc.), technology solutions to implement the design, testing and acceptance criteria, etc. Using the selected technology, MSI will be responsible to develop the registry as per the finalized requirements (please refer to Annexure for detailed requirements) and shall install the same on its own cloud infrastructure. For the operations phase, the MSI will create the SOPs and will follow them to perform the transactions on this registry. The scope of MSI over the entire lifecycle is provided below:

Step	Description
Creation	• MSI will create a user-interface for recording the new registries • MSI will grant access rights to administrators having necessary permissions to perform create transactions • MSI will enter the details about the registries created till the go-live
Read or view	• MSI will enable read/view transactions using open interfaces (Open APIs) • MSI will manage the access rights to administrators having necessary permissions to perform read transaction(s)
Update	• MSI will create a user-interface for recording the update in existing records • MSI will manage the access rights to administrators having necessary permissions to perform update transactions • After the go-live, every time a new registry gets created under the IPeG, the MSI will enter the details about the new registry • In case, there are any changes in details of the registry, MSI will make necessary updates. The MSI will strive to automate this process by creating the other registries in a manner which can facilitate this auto-update on a real-time basis.
Passivation of selected records	• MSI will create a user-interface for passivation/activation of record(s) • MSI will manage the access rights to administrators having necessary permissions to perform activation/passivation transaction(s)

3.2.3.3. Data Sources - Metadata Registry

Over a period of time, as the program gets rolled out, there will be various registries which will contain data about various elements. The metadata registry shall contain list of all the data fields under IPeG program, and brief details about them.

The entire lifecycle of this component has four types of interactions i.e. creation, update, view and passivation. The MSI will be responsible to design, development, install, operation and maintain the registry. As part of the design, the MSI will be responsible to define format, permissible interactions and conditions, interaction mechanisms (APIs), access controls and authorization mechanisms, relationships (parent-child, siblings, etc.), technology solutions to implement the design, testing and acceptance criteria, etc. Using the selected technology, MSI will be responsible to develop the registry as per the finalized requirements (please refer to Annexure for detailed requirements) and shall install the same on its own cloud infrastructure. For the operations phase, the MSI will create the SOPs and will follow them to perform the transactions on this registry. The scope of MSI over the entire lifecycle is provided below:

Step	Description
Creation	• MSI will create a user-interface for recording the new registries • MSI will grant access rights to administrators having necessary permissions to perform create transactions • MSI will enter the details about the registries created till the go-live
Read or view	• MSI will enable read/view transactions using open interfaces (Open APIs) • MSI will manage the access rights to administrators having necessary permissions to perform read transaction(s)
Update	• MSI will create a user-interface for recording the update in existing records • MSI will manage the access rights to administrators having necessary permissions to perform update transactions • After the go-live, every time a new registry gets created under the IPeG, the MSI will enter the details about the new registry • In case, there are any changes in details of the registry, MSI will make necessary updates. The MSI will strive to automate this process by creating the other registries in a manner which can facilitate this auto-update on a real-time basis.
Passivation of selected records	• MSI will create a user-interface for passivation/activation of record(s) • MSI will manage the access rights to administrators having necessary permissions to perform activation/passivation transaction(s)

3.2.3.4. Data Sources – Rules Database

This database will contain all the business rules used across the IPeG components. By encoding all rules into this database, the system will automatically be able to determine whether a request

can be served or not. In case, it can be served then the concerned component(s) of IPeG will be able to handle the request.

One of the key purposes of this database will be to store codified rules as defined in the Data Exchange Framework and Guidelines which will form the basis for Data Exchange Gateway. As soon as, there is a need for different applications under IPeG to obtain the data from data sources, the Data Exchange Gateway will request the business rules database to verify the authorization for this role and applicability of associated rules for this transaction. The rules in database will also govern interactions between different applications under IPeG. The MSI will have to also create an SOP on the major business scenarios which will require interaction of different IPeG application components.

The entire lifecycle of this component has four types of interactions i.e. creation, update, view and passivation. The MSI will be responsible to design, development, install, operation and maintain the database. As part of the design, the MSI will be responsible to define data fields, permissible interactions and conditions, interaction mechanisms (APIs), access controls and authorization mechanisms, relationships (parent-child, siblings, etc.), technology solutions to implement the design, testing and acceptance criteria, etc. Using the selected technology, MSI will be responsible to develop the database as per the finalized requirements (please refer to Annexure for detailed requirements) and shall install the same on its own cloud infrastructure. For the operations phase, the MSI will create the SOPs and will follow them to perform the transactions on this database. The scope of MSI over the entire lifecycle is provided below:

Step	Description
Creation of the Rule database	• MSI will create a user-interface for recording the new rules • MSI will grant access rights to administrators having necessary permissions to perform create transactions • MSI will enter the details about the rules mentioned in the notified Data Exchange Framework Guidelines and detailed out rules during the implementation) • MSI will create the entries of business rules applicable for interactions between various components
Reading or viewing of the rule database	• MSI will enable read/view transactions using open interfaces (Open APIs) • MSI will manage the access rights to administrators having necessary permissions to perform read transaction(s)
Update of the Rule database	The complexity of the rule database is such that it will require constant updates as the IPeG program as a whole matures and different application components including the registries are created and are operational. Thus, the MSI in coordination with CHiPS and the PMU team will have to define standard process, technology interventions to update the rule database. • MSI will create a user-interface for recording the update in existing records • MSI will manage the access rights to administrators having necessary permissions to perform update transactions

Step	Description
	• After the go-live, every time a new rule gets defined under the IPeG, the MSI will enter the details about this in the rules database. • In case, there are any changes in details of the existing rule, MSI will make necessary updates. • MSI will strive to ensure that new or updated rule(s) become applicable on a real-time basis.
Passivation of selected records	As the system evolves there might be a need to passivize certain rules earlier encoded in the rule database. Therefore, the MSI will therefore have to develop standardized technology and process interventions required to passivize records in rule database. • MSI will create a user-interface for passivation/activation of record(s) • MSI will manage the access rights to administrators having necessary permissions to perform activation/passivation transaction(s)

3.2.3.5. Data Sources – Consent Repository

The collection, storage, processing/authentication and exchange of data may require consent from individual to whom the data belongs, depending upon nature of the data being shared and the legal framework governing the same. MeitY has define the electronic consent framework and this framework will be utilized as a benchmark for this repository.

In ideal scenario, all department(s) will maintain consent obtained from citizens in their own records. However, as many departments may not be equipped to maintain the consent, the feature to store obtains and store consent would be made available through consent repository offered under IPeG. Moreover, the consent captured within the IPeG this will be stored by CHiPS in consent repository under IPeG program.

The MSI will develop a consent repository which should have following features:

- consent platform should fully API driven, all functions should expose through APIs making it easy for departments to integrate with consent repository and systems
- should have facility to store and retrieve the specific consent as and when required.
- each consent data should be mapped with a unique ID (SRN ID / Aadhaar reference ID)
- all consent data should be stored with adequate security measure.
- system should capable for handling generation of consent data set required for audit and other references.

Step	Description
Creation	• MSI will create a user-interface and API-interface for recording the new consent • MSI will grant access rights to administrators having necessary permissions to perform create transaction

Step	Description
Read or view	• MSI will enable read/view transactions using open interfaces (Open APIs) • MSI will manage the access rights to administrators having necessary permissions to perform read transaction(s)
Update	• MSI will ensure that the update in existing records is not feasible • MSI will manage the access rights to administrators having necessary permissions to perform update (create new record) transactions • After the go-live, every time a new consent gets captured under the IPeG, the concerned component will store the consent in the consent repository. • MSI will strive to ensure that new consent(s) become applicable on a real-time basis.
Passivation	• MSI will create a user-interface for passivation/activation of record(s) • MSI will manage the access rights to administrators having necessary permissions to perform passivation transaction(s) as per the consent details provided by the citizen

3.2.3.6. Data Sources – Public Service Registry

The government delivers various public services to the citizens. Each of these public services have its unique features i.e. eligibility conditions, application data elements, access points, process, timeline, service levels, fees, consent mechanism, etc. This registry will store the information about these unique features. This registry will be used to respond to citizens enquiry about these public services as well as during the proactive service delivery to the citizens. The typical information stored in public services registry will include the following:

S. No.	Attributes (indicative)	Descriptions
1.	Executing Dept(s)	This is the body that rolls out the scheme in the state. It could be the state department or central agency.
2.	Fund	The amount of money budgeted for a scheme. Typically, as per the executing department and / or the finance department.
3.	Benefit	Details about the benefit.
4.	Eligibility Criteria	This is a set of rules for determining whether a person is eligible for the scheme.
5.	Application Process	Typically, a scheme needs to be applied for via some process. This may include an application form and associated documents. This may be online or offline. The service touchpoint may be via a citizen centre and/or state department.

S. No.	Attributes (indicative)	Descriptions
6.	Supporting documents	These are the set of documents to be submitted with the scheme application.
7.	Validity of scheme	Whether any limited period where one can apply for a scheme
8.	Application Fees	Govt application fees to be paid.
9.	Application Tracking	Process for tracking an application for the citizen.

The major requirements for this registry are as follows:

- The creation, update, activation/passivation should be possible through user interfaces.
- The read/view should be possible through open interfaces (Open APIs).
- The creation, update, activation/passivation transactions should have proper authorization and workflow-based approvals
- As the details are machine readable, all the details should be entered in specified format
- When a scheme is withdrawn or temporarily stopped, it will not be implemented for that period. In such circumstances, it needs to be passivized. The MSI shall make provisions to allow passivizing the scheme through proper workflow-based authorization.
- In rare circumstances, the schemes would need to be merged. The scheme merger shall be provisioned by altering the attributes of schemes like eligibility, benefit amounts or other criteria. This solution should capable to do scheme merger without affecting the data integrity.
- Every public service/scheme shall have a unique ‘Public Service ID’. This ID shall be used to uniquely identify a Public Service under IPeG program.
- When schemes are announced by the Government, there are standard reporting formats prescribed by them. The scheme owner departments shall have to report the implementation details periodically. All such reports shall be automatically generated by the platform with minimal intervention from the scheme owner departments. The features like auto-mailing and messaging needs to be implemented across the standard reporting formats. Further, these features shall be implemented across the platform also.
- The standard reporting formats for all the schemes shall also be stored in this registry and shall be accessed by the platform microservices to serve the platform stakeholders and others.

The scope of work of MSI for development of public service registry can be divided into 4 major pillars.

Step	Description
Creation	• MSI will create a user-interface and API-interface for recording the new public service

Step	Description
	• MSI will grant access rights to administrators having necessary permissions to perform create transaction
Read or view	• MSI will enable read/view transactions using open interfaces (Open APIs) • MSI will manage the access rights to administrators having necessary permissions to perform read transaction(s)
Update	• MSI will create a user-interface for recording the update in existing records • MSI will create a user-interface for merging the existing records (may be used to merge schemes by government) • MSI will manage the access rights to administrators having necessary permissions to perform update transactions • After the go-live, every time a new public service gets captured under the IPeG, the MSI will make an entry in this registry • MSI will strive to ensure that new records(s) become applicable on a real-time basis.
Passivation	• MSI will create a user-interface for passivation/activation of record(s) • MSI will manage the access rights to administrators having necessary permissions to perform passivation/activation transaction(s)

3.2.3.7. Data Sources – Social Registry Number Vault

The IPeG model is based on two ID concept, one foundation ID (Aadhaar) & another functional ID named as Social Registry ID Number (SRN ID). For enabling data exchange between departments (those departments integrated with IPeG ecosystem), SRN ID is required to generate and seed in department databases along with Aadhaar reference ID against each beneficiary. Using SRN as functional ID, data exchange gateway will facilitate the departments for secure information exchange between Information Users (Citizens, Departments, Call Centre Agents, Service Delivery Agents, etc.) and Information Providers (Federated Social Registries, Other Registries) through a pre-defined data exchange rules and protocols.

The SRN Vault for departments should encompass the following events:

i. The SRN vault shall be a central solution for all departments hosted and managed by CHiPS.

ii. The solution should capable of generating SRN ID for each input Aadhaar reference ID and should store both the reference ID & SRN ID centrally.

iii. SRN ID generation mechanism must be a secure solution.

iv. Each SRN ID should be unique in nature and logic should be universal for all the departments.

v. The APIs shall be exposed by the SRN Vault for (a) Generation SRN ID, and (b) Update of the status of SRN ID

vi. The solution should capable of querying SRN ID, which accepts Aadhaar Reference ID as input and returns SRN ID as output.

Apart from meeting the above-mentioned functional requirements, the SRN Vault also ensures the application security, performance of system shall respond fast enough to generate & retrieve SRN ID & it may be scalable enough to support clustered deployment for high availability.

As part of the business and technical services, the MSI will be responsible for the following once the SRN Vault becomes operational:

i. Integration support to the department for availing SRN generator service and storing SRN ID in SRN Vault.

ii. MSI need to generate SRN ID for all the existing Aadhaar Reference Key(s).

iii. MSI should facilitate the department for seeding the SRN ID along with Aadhaar Reference Key in the scheme database(s).

3.2.3.8. Data Sources – Benefit Registry

The benefit registry enables the government to take a comprehensive view of benefits being given to any resident through different schemes. The comprehensive data will result in faster and better decisions in granting the benefit to the resident(s). Other key advantage of benefit registry is department can map the potential beneficiary with their scheme based on beneficiary eligibility and identify the eligible but unregistered potential beneficiaries. The source of data for this registry will be (i) public service registry, and (ii) social registry.

The MSI should consider during development of benefit registry:

- Benefit registry should capable of generating list of left out (eligible but unregistered) beneficiaries so that department can reach out to them for awareness
- Department should be able to perform following activity: (i) Scheme analysis, (ii) Fraud identification, and (iii) Report generation based on different parameter like exiting beneficiary, potential beneficiary, left out beneficiary etc.

The scope of work can be divided into 4 major pillars and overall quality control will however be the responsibility of MSI.

Step	Description
Creation	• MSI will create a user-interface and API-interface for recording the new record(s) • MSI will grant access rights to administrators having necessary permissions to perform create transaction

Step	Description
Read or view	• MSI will enable read/view transactions using open interfaces (Open APIs) • MSI will manage the access rights to administrators having necessary permissions to perform read transaction(s)
Update	• MSI will create a user-interface for recording the update in existing records • MSI will manage the access rights to administrators having necessary permissions to perform update transactions • After the go-live, every time a new public service gets created in the Public Service Registry, the MSI will ensure an entry gets created in this registry • After the go-live, every time a beneficiary gets registered/unregistered in the scheme database, the registry will get updated through the APIs • MSI will strive to ensure that new records(s) become applicable on a real-time basis
Passivation	• MSI will create a user-interface for passivation/activation of record(s) • MSI will manage the access rights to administrators having necessary permissions to perform passivation/activation transaction(s)

3.2.4. Access Channels

3.2.4.1. Access Channels - IPeG Web Portal (Common Services Portal)

At present, there are multiple front-end applications and websites, which the citizen is required to access in order to avail the various services of the government. Moreover, these front-end applications are not accessible through multiple access channels such as web, mobile, service delivery centres, call centre, service delivery outlets, etc.

A web portal shall be implemented as part of IPeG System where all department service delivery application will be integrated. The Web Portal would be available to all stakeholders (residents, government officials, call centre agents, service delivery outlets, etc.) to perform various functions under the public service delivery ecosystem.

Citizen interaction

The citizen will use IPeG Web Portal for the following cases:

- **Scheme Discovery –** To discover the list of all enlisted public services in the State
- **Scheme Eligibility** – To check the eligibility of a citizen for all enlisted public services being delivered in the State
- **Service Application** – Apply for all onboarded public services provided in the State
- **Status check** – To check the status of an applied and onboarded public service
- **Data Correction or Aadhaar seeding** – To update Aadhaar or data in an already availed and onboarded public service

- **Grievance** – To lodge or check the status of a lodged grievance

Government Interaction

The Government officials can use this portal to access the web portal for the following:

- **Data Correction or Aadhaar seeding** – To update Aadhaar or data in an onboarded public service which has been availed by the citizen
- **Service Application Scrutiny** - To scrutinize the submitted application for onboarded service delivery
- **Output Delivery** - To generate certificate (non-DBT scheme), transfer benefit to bank account (cash based DBT scheme), or authenticate beneficiary (in-kind based DBT scheme) of onboarded public service
- **Electronic Document Creation / Conversion:** To generate a new certificate as part of service delivery, or to convert existing paper-based document or electronic non-standardized form into machine readable form
- **Grievance Resolution:** To resolve or monitor the grievance submitted by the citizen

The core objective of web portal is to have various modes of service delivery available for a citizen. The following table defines the services available

Access Channels	Discovery/ Eligibility	Apply (Service)	Status Check	Seeding/ Data Update	Grievance
IPeG Web Portal	Yes	Yes	Yes	Yes	Yes

The key requirements related to Web Portal are mentioned below:

i. The portals should support both English and Hindi languages
ii. The portal should be implemented using a Content Management System to allow authorized users of CHiPS to manage publication of content on the portal.
iii. The portal shall be accessible to all irrespective of technology, platform, devices or disabilities of any kind.
iv. The portal shall adhere to the Web Content Accessibility Guidelines (WCAG 2.0), Guidelines for Indian Government Websites (GIGW) and W3C web content accessibility latest guidelines.
v. The portal should implement basic design principles in portal design including use of consistent, unified common themes including a consistent unique stylesheet including fonts, colours, etc. and implement consistent look and feel and navigation.
vi. The portal should implement a robust security mechanism and proactively monitor the same for improvements.
vii. The portal should be easy to modify as per the usage patterns with minimal technical efforts

viii. The portal should leverage technological advancements for portal applications as they emerge and implement the same.

ix. The portal developed by the MSI must be user friendly and intuitive keeping in mind user convenience

The MSI shall be responsible to ensure, including but not limited to the following:

- **Solution Design:** The MSI will be responsible to gather the detailed requirement for this web portal and prepare the detailed design for this component. The design should cover various usage scenarios, volume estimation, integration with internal and external components, etc.

- **Development, Integration, Installation, Commissioning:** MSI is responsible for development, integration, testing, installation and commissioning of the web portal on its own cloud infrastructure in PaaS model. The proposed database should be an open source solution along with Enterprise support and should be utilized in a PaaS model. The proposed solution should meet the functional requirement specifications and minimum technical specifications as provided in Annexure. MSI shall be responsible to ensure integration, including but not limited to all components of IPeG solution provided by MSI

- **Software Operations and Maintenance:** The MSI shall be responsible for the maintenance of the service which includes but not limited to bug fixes, patch upgradation, performance optimization, etc. The MSI is expected to position appropriate qualified and trained manpower to manage the Web Portal.

- **Provisioning of Licenses:** The MSI will be responsible to provide licenses, as necessary. Thus, the licenses should be sufficient to meet the scaling requirements. The MSI should aim to utilize the latest version, or previous versions (in case of stability issues in latest version) of software. In case, the MSI requires exemption from this, the MSI should request the CHiPS for such an exemption giving clear reasons for this request. In case of any COTS/OTS products, the MSI should follow disciplined approach (as per the best practice defined by the OEM) for configuration and customization which should not restrict CHiPS from utilizing any future upgrades to its solution.

- **Documentation:** The MSI will be responsible to deployed skilled technical staff as part of the technical helpdesk and provide them the requisite training for operation, maintenance, handholding, etc. The functional support and coordination will be carried out by the CHiPS in-house team and MSI will be required to provide them necessary trainings and documentation.

- **Technical Support:** The MSI will be required to provide technical services as described below:
  - Develop the portal's initial content in consultation with CHiPS
  - Train the CHiPS in-house staff to update the content based on requirements. As part of this, MSI shall provide training to 5 users identified by CHiPS on the following:
    - Overview of the CHiPS's Portal Content Management System
    - Portal operations such as upload of content, managing publication, archival, etc.

- **Functional Support (CHiPS In-house Staff)**: The CHiPS in-house staff will carry out the following:
  - review and update of content on the web portal through CMS
  - continuous monitoring of the content to ensure it is up to date

3.2.4.2. Access Channels - IPeG Mobile Application

This mobile application will provide the same range of functionalities as that of the common services portal on mobile platform. It will act like an aggregator wherein all public services of Chhattisgarh can be availed through this single software application for residents. Similarly, government officials can access this application and perform their monitoring and approval duties as per public services allotted to them. The number of public services made available through this application will keep increasing as more and more public services are onboarded to IPeG.

Citizen Interaction

The citizen will use IPeG Mobile App for the following use cases:

- **Scheme Discovery –** To discover the list of all enlisted public services in the State
- **Scheme Eligibility** – To check the eligibility of a citizen for all enlisted public services being delivered in the State
- **Status check** – To check the status of an applied and onboarded public service
- **Data Correction or Aadhaar seeding** – To update Aadhaar or data in an already availed and onboarded public service
- **Grievance** – To lodge or check the status of a lodged grievance

In addition to above, the following feature(s) may be accessible to the citizens at a later date:

- **Service Application** – Apply for all onboarded public services provided in the State

The Government officials can use this portal to access the mobile application for the following:

- **Data Correction or Aadhaar seeding** – To update Aadhaar or data in an already availed public service
- **Service Application Scrutiny** - To scrutinize the submitted application for service delivery
- **Output Delivery** - To generate certificate (non-DBT scheme), transfer benefit to bank account (cash based DBT scheme), or authenticate beneficiary (in-kind based DBT scheme)

- **Electronic Document Creation / Conversion:** To generate a new certificate as part of service delivery, or to convert existing paper-based document or electronic non-standardized form into machine readable form
- **Grievance Resolution:** To resolve or monitor the grievance submitted by the citizen

The core objective of mobile app is to have various modes of service delivery available for a citizen. The following table defines the services available

Access Channels	Discovery/ Eligibility	Apply (Service)	Status Check	Seeding/ Data Update	Grievance
IPeG Mobile App	Yes	Yes	Yes	Yes	Yes

The key requirements related to Mobile application, but not limited to, are mentioned below:

- The mobile application should provide an intuitive and user-friendly GUI that enables users to navigate and apply actions with ease. The GUI should be responsive with very little or no delays or time lag at launch or whilst navigating through screens.
- The mobile application should enable ease of configuration and changes to existing GUIs and support the introduction of new screens.
- The mobile application should provide on screen tips and online help to aid users while interacting with it.
- The mobile application should make use of data available in the existing database and reduce duplicate data entry
- The mobile application should be easily customizable and easy to administer data in the database
- Network level security and traffic should be encrypted using secured connectivity
- The mobile application should structure overall content with proper tagging to make them screen reader friendly.
- The mobile application should ensure compatibility with latest versions of all major mobile operating systems i.e. Android and iOS.
- The mobile application should develop resolution independent design structure i.e. should adjust itself automatically as per the screen resolution, form factor and size of the mobile
- The mobile application should work flawlessly across different platforms
- There should be minimum use flash contents so that home page should be loaded quickly
- The mobile application should provide Role Based Access control
- The mobile application should come with mobile threat prevention and recovery system
- The mobile application should support both English and Hindi language

The MSI shall be responsible to ensure, including but not limited to the following:

- **Solution Design:** The MSI will be responsible to gather the detailed requirement for this mobile application and prepare the detailed design for this component. The design should cover various usage scenarios, volume estimation, integration with internal and external components, etc.

- **Development, Integration, Installation, Commissioning of Platform Service:** MSI is responsible for development, integration, testing, installation and commissioning of the mobile application on mobile application app-stores (e.g. App Store for iOS of Play Store for Android, etc.) and host associated components on its own cloud infrastructure in PaaS model. The proposed database should be an open source solution along with Enterprise support and should be utilized in a PaaS model. The proposed solution should meet the functional requirement specifications and minimum technical specifications as provided in Annexure. MSI shall be responsible to ensure integration, including but not limited to all components of IPeG solution provided by MSI

- **Software Operations and Maintenance:** The MSI shall be responsible for the maintenance of the service which includes but not limited to bug fixes, patch upgradation, performance optimization, etc. The MSI is expected to position appropriate qualified and trained manpower to manage the Mobile Application.

- **Provisioning of Licenses:** The MSI will be responsible to provide licenses, as necessary. Thus, the licenses should be sufficient to meet the scaling requirements. The MSI should aim to utilize the latest version, or previous versions (in case of stability issues in latest version) of software. In case, the MSI requires exemption from this, the MSI should request the CHiPS for such an exemption giving clear reasons for this request. In case of any COTS/OTS products, the MSI should follow disciplined approach (as per the best practice defined by the OEM) for configuration and customization which should not restrict CHiPS from utilizing any future upgrades to its solution. The MSI should ensure that the application is hosted on the Mobile Application Appstore for Android and iOS.

- **Documentation:** The MSI will be responsible to deployed skilled technical staff as part of the technical helpdesk and provide them the requisite training for operation, maintenance, handholding, etc. The functional support and coordination will be carried out by the CHiPS in-house team and MSI will be required to provide them necessary trainings and documentation.

- **Technical Support:** The MSI will be required to provide technical services as described below:
  - Develop the mobile application's initial content in consultation with CHiPS
  - Train the CHiPS in-house staff to update the content based on requirements. As part of this, MSI shall provide training to 5 users identified by CHiPS on the following:
    - Overview of the CHiPS's Content Management Framework
    - Operations such as upload of content, managing publication, archival, etc.

- **Functional Support (CHiPS In-house Staff)**: The CHiPS in-house staff will carry out the following:
  - creation, review and update of content on the mobile application
  - continuous monitoring of the content to ensure it is up to date

3.2.4.3. Access Channels – CG State DBT Portal

This is going to act as a one-stop reporting platform for all Direct Benefit Transfer (DBT) schemes in the state. All departments having DBT schemes can report data here to get an overview on expenditures, beneficiaries, different parameters of DBT enablement, month on month progress etc.

Every state department having a DBT scheme will have login credentials in this portal. CHiPS will have admin rights of this portal and will ensure onboarding, user access and monthly reporting of DBT scheme. Each department will be able to see all data of its own but will be able to see only selective data of other departments.

The key features for DBT portal are as follows:

- Departments can share data with the State DBT portal in three ways and all modes need to be supported by the DBT portal:
  - By logging in directly to the portal and keying in the aggregate statistics of key performance indicators of DBT implementation
  - By bulk upload of an excel file with all aggregate statistics required
  - By sharing data directly from their scheme MIS to the DBT portal through integration APIs provided by DBT portal
- State DBT portal should be integrated with DBT Bharat portal, which is the national portal for reporting DBT progress in all states.
- State DBT portal should provide APIs for integration of department IT systems with it.
- The state DBT portal should have a section(s) dedicated to multiple documents pertaining to latest directives around DBT, meeting proceedings, best practices from around the country and training or capacity building materials on improvement of DBT implementation. There should a facility to add/merge/remove sections on this DBT portal.
- The state DBT portal should allow role-based access to users with single-sign on facility.
- The State DBT portal should be integrated with Policy Planning Tool (Business Intelligence Tool) component of IPeG for reporting and dashboarding. The MSI will be responsible to design and configure the reports on aforementioned tool to view progress department-wise, scheme-wise, district-wise and highlight aggregate statistics at the state level.
- Utilize the Learning Management System component of IPeG for training materials, trainings, assessment, etc.

The MSI shall be responsible to ensure, including but not limited to the following:

- **Solution Design:** The MSI will be responsible to gather the detailed requirement for this web portal and prepare the detailed design for this component. The design should cover various usage scenarios, volume estimation, integration with internal and external components, etc.

- **Development, Integration, Installation, Commissioning of Platform Service:** MSI is responsible for development, integration, testing, installation and commissioning of the web portal on its own cloud infrastructure in PaaS model. The proposed database should be an open source solution along with Enterprise support and should be utilized in a PaaS model. The proposed solution should meet the functional requirement specifications and minimum technical specifications as provided in Annexure. MSI shall be responsible to ensure integration, including but not limited to all components of IPeG solution provided by MSI

- **Software Operations and Maintenance:** The MSI shall be responsible for the maintenance of the service which includes but not limited to bug fixes, patch upgradation, performance optimization, etc. The MSI is expected to position appropriate qualified and trained manpower to manage the DBT Portal.

- **Provisioning of Licenses:** The MSI will be responsible to provide licenses, as necessary. Thus, the licenses should be sufficient to meet the scaling requirements. The MSI should aim to utilize the latest version, or previous versions (in case of stability issues in latest version) of software. In case, the MSI requires exemption from this, the MSI should request the CHiPS for such an exemption giving clear reasons for this request. In case of any COTS/OTS products, the MSI should follow disciplined approach (as per the best practice defined by the OEM) for configuration and customization which should not restrict CHiPS from utilizing any future upgrades to its solution.

- **Training and Documentation:** The MSI will be responsible to deployed skilled technical staff as part of the technical helpdesk and provide them the requisite training for operation, maintenance, handholding, etc. The functional support and coordination will be carried out by the CHiPS in-house team and MSI will be required to provide them necessary trainings and documentation on the train-the-trainer approach. MSI will be required to do (i) Training need assessment, (ii) prepare training plan and content, and (iii) impart trainings and ensure its effectiveness. The trainings should be designed keeping in mind the various roles such as senior officials, department users, field users, admin users, etc.

- **Technical Support:** The MSI will be required to provide technical services as described below:
  - Develop the portal's initial content in consultation with CHiPS
  - Train the CHiPS in-house staff to update the content based on requirements. As part of this, MSI shall provide training to 5 users identified by CHiPS on the following:
    - Overview of the CHiPS's Portal Content Management Framework
    - Portal operations such as upload of content, managing publication, archival, etc.
  - Prepare, update and maintain the documentation related to trainings, user manual, integration manual, etc.
  - As part of technical services provide technical support to the concerned departments which are interested in using the DBT portal. The MSI should plan for nearly 50 schemes.

The final consolidated list would be provided to the MSI in the requirement gathering phase.
    - Monitor the usage and health and provide necessary report(s) and recommendations to CHiPS (on usage and health)

- **Functional Support (CHiPS In-house Staff)**: The CHiPS in-house staff will carry out the following:
    - creation, review and update of content on the portal
    - continuous monitoring of the content to ensure it is up-to-date
    - organizing trainings and workshops for stakeholders and end-users
    - coordination with departments for providing information
    - coordination with CHiPS, Finance Department, Government of India officials, etc. for necessary reports

3.2.4.4. Access Channels - IPeG Call Centre

CHiPS intends to obtain the Call Centre services to enable the government to provide information and resolution of general (non-technical) queries of stakeholders. The Call Centre is required in a managed services model and can be situated in the State of Chhattisgarh. The necessary software, hardware, network, manpower, etc. is to be provided by the MSI on the managed services model. The MSI shall be responsible to provision, operate and maintain the necessary IT and Non-IT infrastructure (Hardware, Software, Manpower) for the call centre services.

IPeG will require an inbound Call Centre. The Call Centre shall act as a touchpoint for interaction of stakeholders with citizens related to entire lifecycle of service delivery i.e. Service Discovery, Service Application, Service Status Check, Service Delivery, and Grievance redressal etc.

The Call Centre is expected to utilize the outgoing facility for the activities, including but not limited to:

- Obtain feedback from citizens on their interaction with the government while availing public services, this will be used on random basis only, as decided by the CHiPS at the time of implementation
- Citizen is discovered to be eligible but unregistered in a particular scheme
- Help citizens lodge grievances pertaining to IPeG onboarded schemes.
- Provide status updates to their service delivery application, preferably as an outgoing voice message in the language of preference opted by the citizens. By default, Hindi will be the language of preference unless otherwise opted by citizen.

For details about the scope related to call centre, please refer to Section 3.6.1 (setup) and Section 3.6.1 (operations). The call centre should be compliant with the requirement and specification provided in the Annexure.

As part of the call centre services, the MSI will be responsible to make available the necessary call centre software(s) including CRM. The main features related to CRM are as follows:

- CRM shall be capable of taking caller satisfaction feedback on SMS. CRM shall be capable of generating SMS in respect of a sample of callers (such as 5th caller who spoke to agent) to get a feedback about quality of response and satisfaction level. The criteria for defining select callers will be as decided by CHiPS from time to time.
- The CRM solution shall support relevant screen pop-ups, to the call centre agent along with the details of the previous calls during the last 30 days, on the agent' desktop on the basis of DNIS (Dialled Number Identification Sequence) etc.
- The CRM solution shall maintain history regarding complaints/grievances using integration with Grievance Toolkit.
- The CRM solution shall support IVR, Voice, Email, FAX, letter and Web based complaint lodging, resolution, and response features using channels such as Voice, SMS, Email, FAX and Web.
- The CRM system should provide analytics and reporting capability on important KPIs concerning all types of users. The CRM system should provide real-time decision support (analytics) to understand customer intentions and customize services and interactions accordingly. For this purpose, the MSI may choose to utilize internal capabilities of CRM or integrate with Advance Analytics Toolkit and generate necessary insights.
- The call centre solution should support call routing functionalities.
- The CRM system should provide a single view of the customer experience and history (customer data integration). The system shall be designed to give a single view of all interactions with a resident for the past 3 months.

3.2.4.5. Access Channels – IT Helpdesk

The helpdesk will be used to address technical queries and tickets raised by the stakeholders. In case of any technical issues, the concerned official will raise a ticket on the helpdesk portal. The Helpdesk is required to be setup in the government's premises situated in Raipur or Nava Raipur, the exact location to be provided to the successful bidder. The necessary software, hardware, network, manpower, etc. is to be provided by the MSI. The MSI shall be responsible to provision, operate and maintain the necessary IT and Non-IT infrastructure (Hardware, Software, Manpower) for the helpdesk services.

The scope of helpdesk (L1, L2 and L3) shall include the entire IPeG solution. The L1 team needs to be onsite in the IT helpdesk, the L2 team can be either onsite or offsite as the team structure proposed by MSI, and the L3 team can be offsite i.e. neither in CHiPS's premise nor in IT Helpdesk premises.

For details about the scope related to helpdesk, please refer to Section 3.7.1 (setup) and Section 3.7.2 (operations). The call centre should be compliant with the requirement and specification provided in the Annexure.

3.2.5. Internal Components

The MSI shall be responsible to ensure, including but not limited to the following:

- **Solution Design:** The MSI will be responsible to gather the detailed requirement and prepare the detailed design for this component. The design should cover various usage scenarios, volume estimation, integration with internal and external components, creation, and maintenance of microservices, etc.

- **Development, Integration, Installation, Commissioning:** MSI is responsible for development, integration, testing, installation and commissioning of the components in a microservices and containerized architecture on its own cloud infrastructure in PaaS model (except Aadhaar Authentication component which will be hosted in State Data Centre). The proposed database should be an open source solution along with Enterprise support and should be utilized in a PaaS model. The proposed solution should meet the functional requirement specifications and minimum technical specifications as provided in Annexure. MSI shall be responsible to ensure integration, including but not limited to all relevant components of IPeG solution provided by MSI

- **Software Operations and Maintenance:** The MSI shall be responsible for the maintenance of the service which includes but not limited to bug fixes, patch upgradation, performance optimization, etc. The MSI should aim to utilize the latest version, or previous versions (in case of stability issues in latest version) of software. In case, the MSI requires exemption from this, the MSI should request the CHiPS for such an exemption giving clear reasons for this request.

- **Provisioning of Licenses:** The MSI will be responsible to provide licenses, as necessary. Thus, the licenses should be sufficient to meet the scaling requirements.

- **Training and Documentation:** The MSI will be responsible to deployed skilled technical staff as part of the technical helpdesk and provide them the requisite training for operation, maintenance, handholding, etc. The MSI will be responsible for preparation of project documentation i.e. user manual, SOPs, etc.

- **Functional and Technical Support:** The MSI will be required to provide functional and technical services as described below:
  - Prepare, update and maintain the documentation.
  - Monitor the usage and health and provide necessary report(s) and recommendations to CHiPS (on usage and health)

3.2.5.1. Internal Components – Enterprise Monitoring System

There will be an Enterprise Monitoring module that would ensure optimal performance of all components of the IPeG project. The module should proactively monitor the performance of components and provide alerts for degradation in performance due to any reason. The performance management would operate on business as well as technical perspectives. Performance monitoring will be an ongoing process and the bidder will have to recalibrate the analysis accordingly. The MSI can aim to leverage the advance analytics tool or provide any specific tool for implementation of this toolkit.

The features of the module from the business perspective should include, but not limited to the following:

- The proposed solution must allow for configuration of business KPIs, integrate data sources for measurement of performance, generate reports and insights (either on its own or through integration with Policy Planning Toolkit or Advanced Analytics Toolkit), define and manage workflows for interventions, trigger notifications (using Messaging service), etc.
- Enterprise monitoring system is required to provide system generated SLA reports along with calculation of penalty as per SLA defined in Volume -3 of the RFP.
- The enterprise monitoring system should be ITIL based including provisions of generating incidence, service request, change request, problem tickets (RCA).

The features of the module from the technology perspective should include, but not limited to the following:

- The proposed solution must be able to perform infrastructure aware application triage, i.e. pinpoint network issues causing application degradation.
- The proposed solution must determine if the root cause of performance issues is inside the monitored application, in connected back-end systems or at the network layer from a single console view
- The proposed solution must proactively monitor 100% of real user transactions; detect failed transactions; gather evidence necessary for triage and diagnosis of problems that affect user experiences and prevent completion of critical business processes
- The proposed solution must provide complete end-to-end transaction visibility by monitoring at a transactional level and without deploying any software at end user desktop.
- The proposed solution must provide a single view that shows entire end-to-end real user transaction and breaks down times spent within the application components, SQL statements, backend systems and external 3rd party systems.
- The proposed solution must be able to provide root-cause probability graphs for performance problems showing the most probable root-cause area within application infrastructure.
- The proposed solution must provide a real-time application topology map to triage and quickly pinpoint the component causing a performance bottleneck in the end-to-end transaction flow.
- The proposed solution must gather available performance indicator metrics from all within real-time production environments and real user transactions 24x7 with minimal overhead on monitored applications without sampling.
- The proposed solution must provide for easy dynamic instrumentation of application code, i.e. be able to enhance out of the box monitoring with extra monitoring definitions
- The proposed solution must allow monitoring granularity of approx. 60 seconds, as least possible for all transactions.

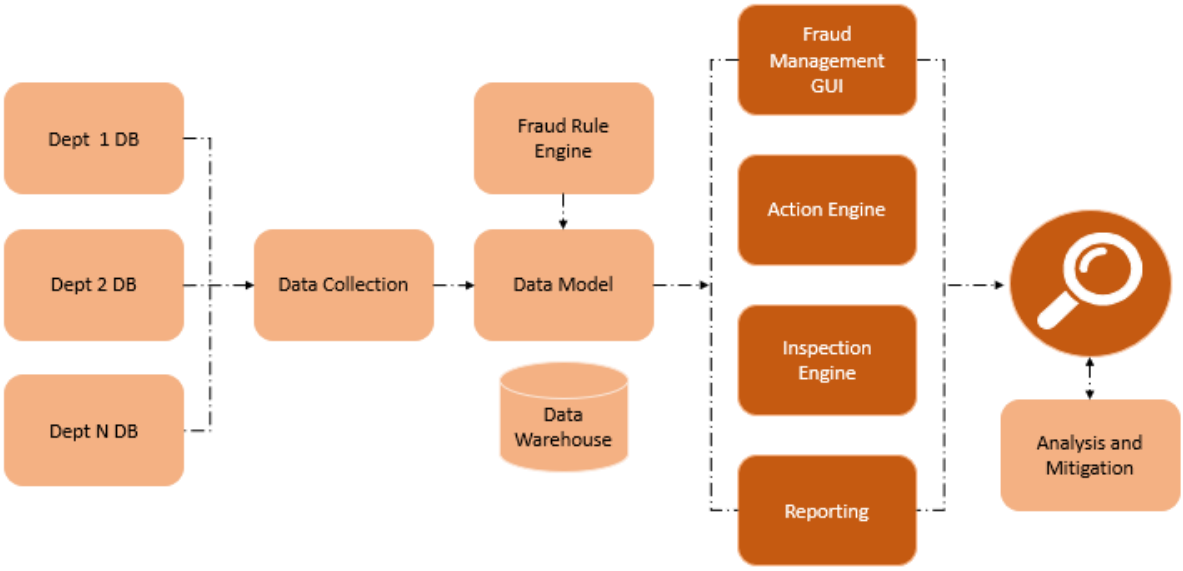
- The proposed solution must provide real-time monitoring of resource utilization like memory usage, DB connection pools and Threads.
- The proposed solution must be able to identify socket and file Input / Output activity from the application.
- As a means of detecting poorly performing SQL, the solution must be able to proactively record all SQL calls, and report on the slow performing ones. The SQL measurements must be made from within the monitored application – not using an external database agent.
- The proposed solution must monitor performance of all stored procedures being executed
- The solution should have provision for automatic transaction discovery, for example by setting up some bounding parameters to describe transactions like the web site, the language, and parameters (such as post, query, and cookies).
- The proposed solution must provide ability to monitor performance of applications up to the method level of execution (Java/.Net method) 24x7 in production environments with negligible impact on monitored application.
- The proposed solution must be able to report on any application errors occurred while executing application functionalities and pinpoint exact place of error within transaction call stack.
- The proposed solution must provide for at least 2 levels of thresholds which can be set on alerts and provide for actions so that alerts can automatically trigger other processes when thresholds are breached. The proposed solution must not necessitate any changes to application source code.
- The proposed solution must proactively identify any thread usage problems within applications and identify stalled (stuck) threads.
- The proposed solution should allow query statement normalization by aggregating hundreds of related query statements into a single performance metric using regular expressions and pattern matching.
- The proposed solution must monitor individual web service and performance transaction debugging for web services. The proposed solution must also monitor web services across multiple processes (cross JVM tracing)
- The proposed solution should eliminate problem resolution guesswork by using its performance metrics to automatically identify complex emerging performance issues, enabling triage and diagnosis teams to solve problems faster and understand their environments better.

3.2.5.2. Internal Components – Performance management & Fraud Detection

Fraud Detection

The objective of the fraud detection system is to ensure that fraudulent transactions are detected and prevented. A fraud detection solution is required to detect and reduce frauds within the IPeG system. The fraud detection solution should be able to detect frauds such as the following:

- Misrepresentation of information;
- Identity theft such authentication as someone else;
- Transactions from outside the state/country;
- Transactions during unusual hours of the day;
- Multiple authentication within very small-time durations;
- Same individual authenticating from different locations;



Possible Components of Fraud Detection Solution

The MSI shall be responsible for creation of fraud scenarios including the above indicative list of frauds. The MSI is encouraged to use modern techniques for fraud detection and fraud detection. The fraud detection solution must have the following characteristics:

- Use of data from different departments: The fraud system will be using data from different departments to corelate and detect frauds
- The high level solution should consist of data management, rule engine, fraud detection GUI, Inspection engine/ analytics engine, etc (eligibility anomaly identification, Network Analytics), Reporting, analysis & mitigation including alert generation,
- Business Rules for Inspection Engine would use algorithms for fraud detection
- The data must be properly profiled cleansed, standardized and finally validated by data quality functions. This exercise will be carried out on each department before doing a matching between the data.
- The data should not be redundant and carry any anomality which are eliminated by means of fuzzy matching.
- A case of fraud detected by the algorithm would need to be manually inspected and then acted upon by an automatic/manual action engine.

- It is important to ensure secure access to the fraud information. For example, the DBA should not be able to read the list of residents who have committed fraud or even delete a record of a resident who has committed fraud.
- The fraud detection system architecture should have a well-defined API for interfacing with other components of IPeG System.
- The fraud detection solution should have a high capacity to handle multiple transactions simultaneously
- A fraud engine should allow setup, configuration and modification of fraud detection rules.
- The fraud engine should update itself based on the frauds detected
- The detection mechanism but not limited to, should be supported - Graph based, Fuzzy matching, etc.
- The fraud detection system should have a workflow management system for fraud detection.
- The cases/ frauds detected is to be managed by the department through alert and case management (Analysis & Management), closing the loop of the process providing the required feedback with their decisions into the system to base the continuous learning process. For this, along with alerts produced, the evidences required by any department to decide on the alert may also be catered along.

Some Key Functional Requirements:

S. No.	Requirement Title
Administrator	
1.	**Manage Users** • The admin should be able to create/add/delete users (business) • The admin should be able to manage user (business) profiles
Technical / Operator	
2.	**Data connections** The user (IPeG operator) should be able to connect the tool to varied data sources (but not limited to), both online and offline/batch, without any programming. Notable connectors include- Cloudera Hadoop, SQL Server, MongoDB, PDF files, Excel files, CSV, APIs etc.
Rule Engine	
3.	• The user should be able to use built-in fraud rules and should also be allowed to integrate and right new algorithms / rules • The user should be able to categorize the rule engine based on the following o rules for updates, o rules for authentication services, o rules for static data, o rules for dynamic data or both, o rules for specific (or linked across) population segments,

S. No.	Requirement Title
	○ rules for specific (or linked across) geographical-social distribution, ○ rules based on transaction types, ○ rules based on risk-based profiles etc. • The user should be able to able to deactivate rules in the rule engine • The user should be able to perform statistical operations for fraud detection • The user should be able to automate and schedule the statistical algorithms and rules to eliminate manual interventions • The user should be able to categorize fraudulent cases based on their severity scores/ levels • The user should be able to publish its outcome of the analysis to the action engine
Action Engine	
4.	• The user should be able to automate the trigger of the event to the field / inspection console on a pre-set rule engine • The user should be able to flag the trigger of the event to the field level to provide the fraud analyst with a precise reason for the case and the trigger that caused the case event • The user should be able to qualify transactions for which cases can be raised, and actions initiated as part of the resolution process • The user should be able to automate the trigger of the event to the field / inspection console on a pre-set rule engine • The user should be able to manually trigger the event to the inspection console with a set of reason for the trigger • The action engine will be able to flag the trigger of the event to the field level/inspection console to provide the fraud analyst with a precise reason for the case and the trigger that caused the case event. • The User will be able to search and view the actions taken (both by the system and recorded by the user) on the case along with current and historical case information. • The user should be able to include suspect records into the caution/blacklist based on automated rule-based strategies or based on manual intervention methods (i.e. update records into the blacklist based on user-initiated action).
Inspection Console - The fraud case management provides the necessary interface for analysis and case resolution functions	
5.	• The user should be able to categories cases for manual inspections using rules, as well as integrated workflow management functionality. • The user should be able to Configure set of rules to identify specific conditions • The user should be able to User defined queues for case handling

S. No.	Requirement Title
6.	The user interface should also provide for: • Users should have the flexibility to automate business functions and processes across the complete lifecycle of a case • Users can define processes and business rules for researching and resolving cases, including investigation resources, time frames, escalation paths and alerts. • The module also acts as a central repository for case histories with centralized auditing capabilities, which can all be viewed online or downloaded in various formats by the authorized users through the user interface component
Reports - The fraud detection module will also provide for a reporting module that is focused on the user and the fraud detection performance	
7.	• The user should be able to extract various from the system. The reports will be available at department, time frame, demographic, scheme levels • Some of the reports that will be available for the users are as follows o Fraud Detection Accuracy Report o Total Fraud Rate o System audit report o Queue status etc. • The user should be able to integrate the data available from the fraud detection system to other reporting and analytics tools available within IPeG • Reporting should provide a robust set of BI and Analytics capabilities enabling different types of users to gain insights from any size of data through data visualization and exploratory analysis. • The solution should help identify patterns, trends and relationships in data that were not evident before.
Non-functional requirements	
8.	**Secure Access** The system should ensure secure access to the fraud information; for example, the DBA should not be able to read the list of residents who have committed fraud or even delete a record of a resident who has committed fraud
9.	**Large Scale Data Handling** The fraud detection system should be capable of handling huge volumes of data coming from enrolment, authentication, logs and BI data stores.
10.	**Rule Management** A fraud engine should allow set up and configuration of fraud detection rules
11.	**Self-Learning** The fraud engine should be a learning system i.e. should update its knowledge based on detection of frauds.

Performance management

For the performance management some of the KPI's, including but not limited to, that will be monitored are:

- Descriptive
  - SLA monitoring – approval, rejection, delivery etc.
  - Sub SLA monitoring
- Diagnostic
  - Reasons for SLA breach if any
  - Correlation to other variables and factors e.g. number of employees, number of service requests, etc.

Scheme Tracking & Monitoring: -

- **Service Level Tracking –**The Platform should allow 'On-the-fly' hierarchy creation for adding drill-down capabilities to visualizations and reports for SLA to Sub-SLA Level of tracking.
- **SLA & Sub SLA Level Tracking** – The platform should be able to track Scheme implementation performance at each task level in detail.
- **Beneficiary Analytics** – The platform should have capability of filtering and clustering the beneficiaries of each scheme and perform subsequent analysis for department to server them better services in timely manner.

State Level Tracking:

- **Registration Monitoring –** Overall Citizen Registration across Schemes to be monitored and tracked the registration trends etc.
- **Micro Cluster based Location Analytics** – The platform should provide Geographical map views (Choropleths, custom conditional highlighting) to provide a quick understanding of geospatial data.

3.2.5.3. Internal Components – Aadhaar Authentication

CHiPS will provide this component and role of the MSI will be limited to integration with authentication platform service and its utilization in this solution.

3.2.5.4. Internal Components – Aadhaar Service Agency

CHiPS is acting as AUA/KUA for Aadhaar authentication and Availing services from CSC for ASA services. Bidder need to propose additional ASA as fallback ASA for smooth operation.

The MSI shall be responsible for following activities for ASA services-

- Integration support for ASA in existing CHiPS Aadhaar Authentication ecosystem
- Minimum per transaction cost for Yes/ No Authentication & e KYC authentication.

3.2.5.5. Internal Components – Data Exchange Gateway

This application should have following features:

- It should support data discovery as a service
- Provision for data extraction / fetching using data virtualization layer in order to process data by combining data from social registries and other data sources.
- API's Integration from where data needs to be fetched.
- Developing business rule for enabling fetch data services
- This application should capable to authenticate the genuine source of request, and it has received through proper from proper channel.
- Enabling data fetch services using SRN ID.
- Ensuring encryption and decryption processes during fetch data services

IPeG needs to harness maximum value from a large amount of data that is generated by implementing various schemes on it. For the schemes to work in cohesion and generate useful data, all the scheme owners should be able to exchange data in a standardized way and avoid ad hoc interfaces and their implementations. Hence, the need for a Data Exchange Gateway. The Data Exchange Gateway is a set of services that enables the consumption of data by the IPeG platform/scheme owner departments from one or more Resource Servers, based on explicit consent obtained from the Provider of the resources.

The MSI may preferably use open-source data exchange frameworks like Open Sabre, IUDX, etc. for the implementation of the Data Exchange platform under IPeG. The Data Exchange Gateway shall have three main components – Catalogue services, Authorization services, and Resource access services.

- Catalogue service that shall provide a framework to manage meta-information about the data
- Authorization service that shall manage authorization to access the data
- Data Access service that shall provide a standardized way to access data

Roles and Responsibilities of entities in Data Exchange Reference Architecture

The entities of the DX architecture, their semantics, roles, and responsibilities are explained in table below.

S. No	Term	Role	Responsibility
1	Provider	Legal Entity	Human, organization or an organizational role that has a responsibility to provide authorization to use resources
2	RS (Resource Server)	Service	Serves resources to authorized Apps / Consumers.
3	Consumer	Legal Entity	Human or Organization that consumes a resource.
4	App	Application	A Consumer's application that consumes resources. Can be a mobile app, web app or server app

S. No	Term	Role	Responsibility
5	Provider App	Application	Helper app used by Providers to manage interactions with the data exchange (manages meta-data and access control). It can be a mobile app, web app or server app.
6	Data Exchange Framework	Service	Hosts and manages meta-data about resources and manages authorization for accessing the resources.
7	Consent	Service	Provider's freely given, specific and informed agreement to accessing and processing of specific resources in their responsibility.
8	Consent Artefact		A machine-readable electronic document that specifies the parameters and scope of data sharing that a Provider consents to, in any data sharing transaction.
9	Personally, Identifiable Information (PII)		Any information that (a) can be used to identify the PII principal to whom such information relates, or (b) is or might be directly or indirectly linked to a PII Principal
10	PII (Personally Identifiable Information) Principal		The natural person to whom the personally identifiable information (PII) relates.
11	Authorization Token		A digital entity that is used to present the authorization credentials to the Resource Server.
12	Catalogue		A registry of meta-data about the resources in the data exchange available for consumption
13	Resource-item		An entry in the Catalogue that describes the meta-information of the resource that is hosted in an associated Resource Server
14	DX (Data Exchange) Authorization Service		AS (Authorization Service) of the data exchange
15	DX (Data Exchange) Catalogue Service		Catalogue Service of the data exchange

S. No	Term	Role	Responsibility
16	DX (Data Exchange) Adapter		Adapter service in front of a Non-DX compliant Resource Server
17	DX (Data Exchange) Administrator	Legal Entity	Responsible foradministering, managing and running the data exchange
18	DX (Data Exchange) CA (Certificate Authority)	Service	Certificate Authority service run by the DX

Resources, managed by a Provider, are hosted on one or more Resource Servers, and are made available for consumption to entities via a description of its meta-information (like its format, Provider, etc.), through a catalogue in the Data Exchange. The Catalogue is both human readable as well as machine-readable.

The Provider registers manages the meta-data of its resources and their associated access control policies via the management interface of the data exchange. The Provider may use a helper application, like the Provider App to register and manage the meta-data and access controls.

The App can register with the Data Exchange to get notified about any changes to the metadata of the resources of interest to the Consumer. The App obtains consent to consume the resources via the authorization interface by obtaining an Authorization Token. This application should capable to authenticate the genuine source of request, and it has received through proper from proper channel.

Any request to a provider's resource by a Consumer App will be checked against the existing access control policies. If no decision can be made, the Data Exchange will coordinate between the Provider and the Consumer to complete a consent transaction and generate the Consent Artefact. The Consent Artefact will be used to update the access control policy for those resources.

The Consumer App can register with the Data Exchange to get notified about any changes to the meta-data.

The envisioned solution should encompass the following events:

- Data exchange catalogue should be a store of meta-information associated with the data assets/resources available with the data exchange
- The Catalogue should be both human readable as well as machine-readable.
- The platform should support data discovery as a service
- The platform should provision for data extraction / fetching using Data virtualization layer in order to process data by combining data form social registries and other data sources.

- The platform should allow the data providers (departments) to manage the meta-data of its resources and their associated access control policies via the management interface of the data exchange
- The platform should have a robust business rule engine for data exchange
- This platform should capable to authenticate the genuine source of request along with proper channel.
- The platform should be capable to exchanging data resources through API's
- The platform should be able to integrate with other IPeG components like Fetch data , anonymization service , translation service etc.
- The platform should enable data exchange services using SRN ID.
- The platform should ensure that it follows encryption and decryption processes during data exchange

Once the Data Exchange Gateway is ready the bidder needs to provide integration and operational support to participant departments for participating in data exchange. Below are some scope which need to be carried out as part of technical services:

- Integration support to the departments for participating in the data exchange framework.
- Facilitating the departments to onboard in the Data exchange framework as Data provider and/or data Requestor.
- Provide support for addressing the data Interoperability issues which may come during data exchange e.g. Trigger & subscription services.
- Provision for data extraction / fetching using data virtualization layer in order to process data by combining data form social registries and other data sources.
- Link and names of portals from where data need to be fetched by writing code.
- Names of various indicators for which data needs to be collected.
- API's Integration from where data needs to be fetched.
- Developing Business rule for enabling fetch data services

3.3. Project Implementation Services

3.3.1. Team Mobilization, Project Initiation, Planning

The MSI needs to plan all the important tasks to ensure that all pre-requisite is met, and the MSI team is able to deliver the project as per the timelines, requirements and service levels. During the course of project, the MSI would be required to prepare project plan, project initiation document, progress reports, risk register, issue register and other project management related documents. The indicative list of project management documents would include the following:

- **Project Schedule**: A detailed week-wise timeline indicating various activities to be performed along with completion dates for the same shall be provided by the MSI.
- **Project Initiation Report**: The project initiation report shall be prepared by the MSI after the initiation of the project. The report shall contain manpower deployment plan, project plan, risk mitigation plan, escalation matrix, etc.
- **Progress Reports**: Detailed weekly, fortnightly, monthly Progress Report along with issues/ escalations/ risks. The format shall be finalized by the CHiPS prior to start of the project.

- **Risk Register:** MSI shall be required to maintain a risk register which shall enlist all possible risks which shall impact IPeG project along with their occurrence and likelihood. The MSI shall also propose the mechanism to mitigate the identified risks.

3.3.2. Requirement Gathering

The MSI shall carry out a detailed assessment to prepare the Functional Requirements Specifications provided in this RFP and formulate the System Requirements Specifications (SRS) document incorporating the requirements provided by all the stakeholders for the implementation of IPeG project.

The MSI will have to complete the hardware & infrastructure sizing exercise after gathering the requirements and will provide detailed Infrastructure Requirement List/Form, deployment architecture and any other required information. CHiPS would validate, procure and commission the infrastructure.

The indicative deliverables under this item shall be:

- Revise Functional Requirement Specification (FRS)
- Software Requirement Specification (SRS) covering the functional requirements, data integration requirements, data management requirements, non-functional requirements, etc.
- Requirement Traceability Matrix
- Gap Assessment Report

3.3.3. Solution Design and Solution Architecture

During this phase, the MSI shall develop a detailed design document that shall meet the requirements captured in the previous phase. MSI during this phase shall be required to perform at least the below mentioned activities:

- Preparation of IPeG Solution Architecture specifying the Functional Architecture, Data Architecture, Deployment Architecture, Network Architecture and Security Architecture
- Preparation of IPeG System Design Document specifying the construction details of the system, each system component's interaction with other components and external systems, and the interface that allows end users to operate the system and its functions
- Development of Security Plan, Business Continuity Plan
- Preparation of data integration and data quality design document specifying how data from desperate source systems shall be integrated in the IPeG
- Dashboard and MIS Report design
- Exceptions and Business Alerts definitions

The illustrative deliverables for these activities are mentioned below.

- Solution Design and Architecture Document (including ER Diagram and Data Flow Diagram)
- High Level Design Document and Low-Level Design Document (including Schema Diagram)
- Detailed Solution Architecture, including:
    - Application architecture
    - Data flow architecture
    - Enterprise architecture
    - User interface (web portals)
    - Database structures
    - Security architecture o Integration architectures
    - Network architecture
- Use Cases
- Application delivery checklist
- UI/UX prototypes and wireframes
- Test Plan
- All Policy, Plan & Methodology Documents covering aspects mentioned above

3.3.4. Software Development, Customization and Integration

The MSI shall develop the software in accordance with the approved requirement specifications, design specifications, and according to the project plan and carry out the unit testing of the software in accordance with the approved test plans. The overall IPeG setup shall be implemented in following environments:

- Development environment
- Testing environment/UAT environment/ Pre-Production/Staging environment
- Sandbox (for API deployment)
- Production environment

The MSI needs to provide software configuration, customization and installation reports to CHiPS. In case of any COTS products, the MSI should follow disciplined approach (as per the best practice defined by the OEM) for configuration and customization which should not restrict CHiPS for any future upgrades to its solution.

The MSI should ensure solution sustainability to meet all RFP requirements, any additional procurement required will have to be taken by the MSI with no additional cost to CHiPS. Other related requirements are mentioned below:

- The application software developed by the MSI has to be user friendly so that users can access it without having extensive training.
- The lifecycle for each phase should be independent, i.e. different teams should work in parallel to complete the track activities per the given timelines.
- The MSI shall also supply any other tools required to complete the integrated solution requirements.
- For the integrated solution, the MSI shall supply:
    - Software and licenses

- Tools, documentation and prepare a list of items supplied. Tools shall be part of the solution. MSI should provide technologies matrix.
- Supply latest supported version of all software to support the solution and any other software, tools and bolt-on/add-on application.
- System Documentation both in hard copy and soft copy.

Note: All licenses supplied by the MSI for the purpose of this project shall be perpetual in nature and shall be in the name of CHiPS.

The deliverables for this activity are mentioned below:

- Development/Customization and Integration of all components of IPeG
- Delivery of software along with Licenses, Operational/ Technical manuals, Library Files, Setup Programs, etc.
- Unit and integration testing results

3.3.5. Solution Testing

The MSI shall provide the testing strategy including traceability matrix, test cases and shall conduct the testing of various components of the software developed/customized. A comprehensive system should be set up that would have the capability to log and track the testing results, upload and maintain the test cases and log and track issues/bugs identified.

The table below depicts the details for the various kinds of testing activities required for each phase of the project:

#	Type of Testing	Responsibility	Scope of Work
1.	System Testing	MSI	1. The MSI shall prepare a test plan as well as test cases and maintain it. The CHiPS may request the MSI to share the test cases and results, if required. 2. The testing should be performed through manual as well as automated methods 3. Automation testing tools will need to be provided by the MSI 4. Comprehensive System testing would be performed for each phase of the application development.
2.	Integration Testing	MSI	1. The MSI shall prepare the Integration test plans and test cases 2. The MSI shall perform Integration testing 3. Integration testing will need to be performed through manual as well as automated methods

#	Type of Testing	Responsibility	Scope of Work
			4. Automation testing tools will have to be provided by the MSI 5. Integration testing would include all data exchanged between various stakeholders 6. Integration testing would be performed for each phase of the application development.
3.	Security Testing (including Penetration and Vulnerability testing)	• MSI • CHiPS or third party appointed by the CHiPS	1. The solution should demonstrate compliance with security requirements as mentioned in this RFP including but not limited to security controls in the application, network layer, and security monitoring systems deployed by the MSI. 2. All IPeG system shall have to pass vulnerability and penetration testing for rollout of each major version. The solution should pass web application security testing for the portal and security configuration review of the baseline infrastructure. 3. An agency appointed by the CHiPS shall carry out security and vulnerability testing on the developed IPeG System. The MSI shall be responsible to address the identified issues. The agency shall cross verify that identified security issues have been properly addressed and have not resulted in new issues. 4. Security testing will need to be carried out in the exact same environment/architecture as the one set up for production. 5. Security test reports and test cases should be shared with the CHiPS, if required 6. Testing tools if required, will have to be provided by the MSI. 7. During the O&M phase, vulnerability assessment and penetration testing will need to be conducted on a yearly basis.
4.	User Acceptance Testing	CHiPS or third party appointed by the CHiPS	1. CHiPS may perform User Acceptance Testing 2. The MSI will need to prepare the User Acceptance Testing test cases

#	Type of Testing	Responsibility	Scope of Work
			3. UAT will have to be carried out in the exact same environment/architecture as the one set up for Production 4. The MSI should fix bugs and issues raised during UAT and seek approval on the fixes from the CHiPS 5. Changes in the application as an outcome of UAT shall not be considered as a Change Request. The MSI will need to rectify the observations raised.

- The MSI needs to provide the details of the testing strategy in its technical proposal including details of intended tools/environment to be used by the MSI for testing
- The MSI must ensure deployment of necessary resources and tools during the testing phases. The MSI shall perform the testing of the solution based on the approved test plan, document the results and shall fix the bugs found during the testing. It is the responsibility of the MSI to ensure that the end product delivered by the MSI meets all the requirements specified in the RFP. The MSI shall take remedial action based on outcome of the tests.
- All tools/environment required for testing shall be provided by the MSI.
- Post Go-Live, the production environment should not be used for testing and training purpose. If any production data is used for testing, it should be masked and it should be protected.
- The necessary changes to meet the requirements shall be carried out by the MSI

The deliverables for this activity are mentioned below:

- Refined Test Plan
- Refined Test Design
- Final Test Case Specification
- Test Data
- Testing Reports
- Necessary modification in software for passing the UAT

3.3.6. Application Certification and Security Audit

IPeG applications need to be certified by the audit and certification agency (such as STQC, CERT -In) before it is deployed into the production environment. During the project, it is expected that several such tests/ audits will be carried out to not only ensure the conformance of the solution provided by the MSI with the scope of work as detailed in this RFP but also to ensure that the platform is implemented in the best of ways to meet the requirements of the Department. The audits will be carried out by a third-party testing/ audit agency identified by CHiPS. MSI shall provide all support for conducting any such audits and comply with the directives that may be given by the third-party auditor. Any audit, vulnerability assessment and penetration testing

(VAPT) or other security tests that are conducted shall be organized and the costs borne by the CHiPS. However, after the audit/ tests are conducted and observations are provided by the third-party testing agency, the MSI shall implement all such changes into the system and re-submit for the repeat audit/ tests. The MSI shall be responsible for making all such changes any number of times until the VAPT, third party testing and audits are completed without any defects and only after the third-party testing agency has certified that the system can go-live, shall the particular application under IPeG be deployed in the production environment.

CHiPS will establish appropriate processes for notifying the MSI of any shortcomings from defined requirements at the earliest instance after noticing the same to enable the MSI to take corrective action. All gaps identified shall be addressed by the MSI at the earliest. It is the responsibility of the MSI to take any corrective action required to remove all shortcomings. It is to be noted that the involvement of the third-party testing agency for acceptance testing and certification and conducting of VAPT, does not absolve the MSI of his responsibilities to meet all SLAs as laid out in this RFP.

The MSI should facilitate or support all the audit requirements through the following:

- Recording details of each user action like successful logins, failed logins, starting a transaction (e.g. entry of an issue), failed attempts to start transactions (i.e. prevented by the user's role/profile), automatic locking a user's account because of multiple failed logins, recognizing and generating alerts for logins from multiple devices, creation of new roles/profiles and changes in user master records.
- IPeG platform should have a provision for automated maintenance of audit trails for all critical user actions and subsequent access of the audit trails by authorized users of the Department for investigation/ forensics.
- Configuring the security audit log to meet the control/security/audit requirements of the Department.
- Configuring the following based on the requirements
    - Auditing procedures and documentation
    - Auditing evaluations
    - Audit data downloads
- Configuring/designing audit trails for business audits and systems audits.
- Audit trails incorporating changes like authorizations, profiles and user master records

3.3.7. Training and Capacity Building

During implementation and operation of IPeG, MSI shall be required to conduct training to ensure successful implementation and operations of the required system. The following shall be responsibilities of the MSI for training:

3.3.7.1. Training Needs Assessment

MSI in consultation with the CHiPS shall identify the training required to be imparted to different stakeholders for successful implementation and operations of IPeG system. The manpower to be trained shall be identified by the CHiPS in consultation with the MSI. The indicative number of resources required to be trained would include representatives from Manufactories, Wholesalers, Retailers as well as officials from the CHiPS, and is tabulated in Subsection titled 'Impart Training'.

3.3.7.2. Preparation of Training Plan

Post identification of the training needs, MSI shall prepare a training plan that highlights training type, target trainees, date of training, venue for training, trainer details, agenda of training etc.

3.3.7.3. Impart Training

The MSI shall impart training to the users catering to the groups tabulated above and has to submit the detailed training plan to the CHiPS as per the timelines mentioned in the RFP.

The MSI shall provide training to all stakeholders, including the application users to efficiently and effectively use the system. Training manuals shall be provided by the MSI. The training shall be grouped module-wise for hands-on training in batches per day for a specified duration/ number of working days. The key trainings have been classified in the table below:

S. No.	Training	Training content outline (Indicative)
1.	Project Sensitization and IT Processes Training	• Objectives, Vision and Mission of the project • Overview of various modules, platform components, toolkits, and microservices • Fixation of Roles and Responsibilities - Overview of workflows • Introduction and Benefits of IPeG IT system • Overview of IPeG architecture • Integration with external scheme owners and service delivery
2.	Database Schemas and Administration Training	• IPeG database architecture • The database schema, masters, transaction tables and views including graph databases • Database Management and Administration for IPeG system • Database Security Controls and definition of roles
3.	Training for Administrative Users	The MSI will have to prepare the list of trainings required for administrative users for various components. The CHiPS will review the list of trainings and accordingly the MSI will be required to conduct the trainings. For each component, the MSI will train nearly 100 administrative users (and CHiPS in-house staff) in batch 50 each in the train-the-trainer mode. The duration of the training will depend on the

S. No.	Training	Training content outline (Indicative)
		duration of content and sufficient time to obtain full understanding of the roles and responsibilities.
4.	Training for End- Users	The MSI will have to prepare the list of trainings required for end users for various components. The CHiPS will review the list of trainings and accordingly the MSI will be required to conduct the trainings. For each component, the MSI will train nearly 25 administrative users (and CHiPS in-house staff) in one-batch in the train-the-trainer mode. The duration of the training will depend on the duration of content and sufficient time to obtain in-depth understanding of the roles and responsibilities and enablement of master trainers to impart training to end-users.

MSI shall also be responsible for re-training the above personnel whenever changes are made to the IT application and the release of screenshot-based documentation in the help mode of the application.

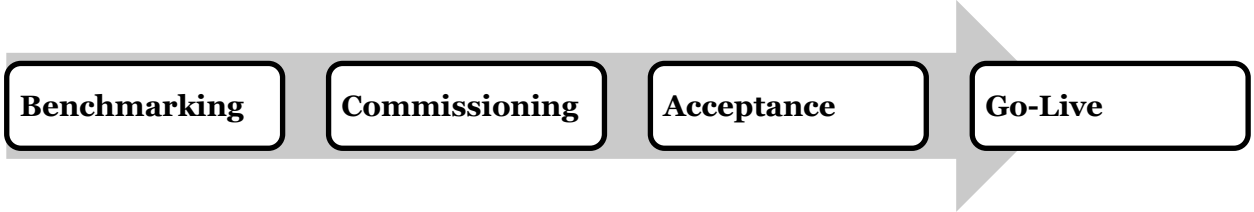
MSI is required to provide a Workshop or Trainings completion report. It should include details of various participants in trainings or workshops and feedback formats.

The deliverables for this activity are mentioned below:

- Training requirement analysis
- Training plan
- Training content and material
- Training completion report

3.4. Benchmarking, Commission, Acceptance and Go-Live

Prior to Go-Live of the IPeG, MSI shall be responsible for undertaking a benchmarking exercise, commission the IPeG and support the CHiPS in User Acceptance testing as shown in the figure below.



3.4.1. Benchmarking

The Benchmarking exercise is intended to evaluate the ability of the proposed IPeG system to scale to the intended usage. It is envisaged to cover the entire IPeG, including but not limited to its applications/software, hosting, other component solutions and all related interfaces. The Benchmarking process does not intend to simulate all the aspects of IPeG, however all design parameters, components and related interfaces shall be considered.

(i) Benchmarking shall be in accordance with the production deployment and solution architecture proposed in the Technical Proposal of the MSI.

(ii) MSI shall be responsible to undertake the benchmarking of the IPeG solution. The MSI shall:

a. Prepare benchmarking test cases and obtain sign-off on the test cases from the CHiPS
b. Supply, build, commission, configure, tune and execute the benchmarks on the cloud environment
c. Provide the tools (load generator), scripts for etc. for benchmarking.
d. Create test data
e. Demonstrate at least one successful (live) run
f. Undertake benchmarking of the IPeG System as per the target parameters mentioned in the SLA given in Volume-I of the RFP.
g. Report the benchmarking output in the format specified by CHiPS or its appointed agency. Key guidelines for reporting benchmarking output are as follows:
    - Reports for resource usage should have graphs with a sampling interval of 3 minutes for all resources (all servers, routers, switches, disk arrays, firewalls etc.)
    - Response Time Reports should include minimum, maximum, average and 90 percentile response times. Response Time should be shown as a function of time for the duration of the test.
    - The test results should also include the iterative configuration changes/tuning required to achieve the benchmark results.
    - The list of cloud and software used for the test shall be the same as proposed by the MSI, if however there is a shortfall in the quantity of the equipment proposed, the MSI shall provide the required quantity of equipment/licenses as the case may-be to achieve the benchmark results and SLA.
h. CHiPS shall witness the benchmark or appoint an agency at its own cost to verify and validate the benchmarking environment and certify the results of the benchmarking. Benchmark test report provided by the MSI shall be verified and certified by the CHiPS

(iii) In the event the solution and the corresponding Bill of Materials proposed by the MSI fails to meet the benchmarking performance criteria, MSI shall enhance/augment and supply additional components (including cloud infrastructure, licenses, etc.) without any additional cost to the CHiPS such that the benchmark performance is delivered by the solution proposed.

(iv) The MSI is expected to define parameters to measure performance of IPeG System in consultation with the CHiPS.

3.4.2. Commissioning

After successful benchmarking of IPeG system, the MSI shall commission the entire system (except Aadhaar Authentication and Aadhaar Data Vault) in its cloud infrastructure. Moreover, the MSI shall commission the Aadhaar Authentication and Aadhaar Data Vault components in the infrastructure (hardware, software, network) provided by CHiPS at the State Data Centre.

The following shall be the key responsibilities of MSI for completion of commissioning:

- Configuration of all the components of the cloud, hardware, software, devices, accessories, etc.
- Integrated testing of all components
- Tuning and testing of application at the Cloud as well as SDC.
- Successful testing of the integrated solution.

3.4.3. Acceptance and Go-Live

Post successful commission of the IPeG System, the CHiPS shall undertake a user acceptance of the entire system. Acceptance for the IPeG System can be divided into the following phases:

3.4.3.1. Pre-Acceptance phase

3.4.3.1.1. Creation of Acceptance Plan

(i) The MSI shall first identify areas of acceptance of the IPeG System. The MSI shall then prepare a draft acceptance plan comprising of acceptance methodology for identified areas, test schedule, timeline of acceptance testing activities and deliverable due dates. The test schedule prepared should identify major test areas, test execution, and test reporting activities. As a part of acceptance plan, MSI will also identify roles and responsibilities of the individuals to carry out the acceptance.

(ii) Acceptance plan should be in alignment with the overall project plan. It will enable MSI and CHiPS to plan the overall project timelines and resource requirements for acceptance phase.

3.4.3.1.2. Assistance in formulating detailed acceptance criteria

(i) MSI shall prepare draft acceptance criteria for each of the above-mentioned areas of acceptance. Acceptance criterion prepared should be in accordance with the system specifications and functional specifications of the products/service.

3.4.3.1.3. Preparation of detailed Pre-Acceptance and Acceptance checklists

(i) MSI shall prepare a detailed checklist of the activities and pre-requisites that are required to be completed before and during the phase of acceptance by CHiPS. This shall include, but are not limited to:

- Required approvals
- Availability of testing tools, monitoring tool and test management tools
- Preparation of acceptance test scenarios, test cases and test data
- Setup of hardware and software etc.

(ii) The test cases and scenarios developed should be well documented in the format approved by the CHiPS.

3.4.3.1.4. Preparation of required environment and facilities

The MSI shall be responsible for setting up the test environment. The test environment, including hardware / software to be tested and support hardware/software, should be as per the planned configuration.

3.4.3.2. Acceptance Phase

3.4.3.2.1. Execution of Tests

(i) MSI shall assist the CHiPS's acceptance test team in executing the defined test cases and scenarios. In the event of unexpected test results / bugs, MSI shall log tickets according to the severity of the issue.

(ii) CHiPS may take assistance from an Agency for support in activities related to acceptance of IPeG System. The MSI must provide all necessary support to the agency for undertaking the acceptance including sharing of system specifications, functional specifications, acceptance plan, and test cases.

3.4.3.2.2. Resolution of issues identified during the acceptance testing

(i) All issues and defects identified by CHiPS's acceptance test team will be recorded in defined template. For each incident, the MSI's defect tracking system should document each issue/defect identified, how it occurred, when it occurred, the tester who discovered it, what system baseline was being used, and a preliminary assessment of the severity

(ii) The MSI should track and report on open defects until they are closed.

(iii) The MSI shall undertake following activities for root cause analysis and take preventive measures:

a. For every defect reported, the MSI team shall carry out root cause analysis and document the same.

b. At agreed upon intervals, the CHiPS's acceptance team and MSI's team should meet to review the identified defects and decide upon their prioritization and disposition.

c. MSI shall undertake remedial actions for resolution of the defect

d. MSI shall work out the preventive measures so that the incident does not occur in the future.

(iv) A sample template for reporting the defects shall be prepared by MSI:

(v) Upon resolution of defects and internal testing, for a maximum of three iterations, the MSI shall be responsible for retesting of the issues at no additional cost. The MSI shall support the CHiPS's acceptance test team in re-executing the acceptance test procedures and retest each corrected defect. CHiPS's acceptance test team can also undertake additional testing if required. If the incident does not re-occur the CHiPS's acceptance test team shall recommend closure of the defect. In case incident continues to occur, the CHiPS's acceptance test team shall inform the MSI and the defect shall remain open.

3.4.3.3. Post Acceptance Phase

3.4.3.3.1. Acceptance Documentation and Signoff

(i) The MSI shall assist CHiPS's acceptance test team in creating the reports for acceptance testing. The reports shall summarize the test activities, and identify outstanding deficiencies and issues.

(ii) The Acceptance Test Final Report shall be the detailed record of the acceptance test activities. It shall record which tests were performed, the pass/fail status of each test, and the discrepancies or issues found.

(iii) MSI shall be responsible for the following deliverables at the end of acceptance testing:

a. Acceptance Test Plan

b. Acceptance Test Schedule

c. Acceptance Test Environment Inventory

d. Acceptance Test Summary Report

e. Acceptance Test Final Report

3.4.3.3.2. Go-Live

Post completion of required documentation and due diligence, MSI shall obtain signoff from the CHiPS's acceptance test team. **This will constitute Go-Live.**

3.4.3.3.3. Final Go-Live

Post completion of required documentation, STQC certification and security audit, MSI shall obtain signoff from the CHiPS's acceptance test team. **This will constitute Final Go-Live.**

3.5. Operations and Maintenance

3.5.1. Software Operations and Maintenance

3.5.1.1. Software Support and Maintenance

IPeG system maintenance and management support includes, troubleshooting and addressing functionality/availability and performance issues and also implementing change requests, license management, updated and upgrades, etc. The activities for software support and maintenance are as follows:

1. The MSI shall provide continuous support through on-site team, telephone, E-mail, Video conferencing, installation visits as required.
2. The MSI shall address all the errors/bugs/gaps in the functionalities of the solution vis-à-vis the signed-off FRS and SRS at no additional cost during the maintenance and management phase.
3. All patches and upgrades from OEMs shall be implemented by the MSI. Technical upgrades of installation to the new version, as and when required, shall be done by the MSI. Any version upgrades of the software/tool/application will be done by the MSI after seeking prior approval from the CHiPS and submitting the impact assessment of any upgrade.
4. O&M team of MSI is expected to onboard any new scheme identified during the O&M period without any additional cost to CHiPS.
5. Any changes/upgrades to the software performed during the support phase shall be subject to comprehensive and integrated testing by the MSI in order to ensure that the changes implemented in the system meet the specified requirements and do not impact

any other existing functions of the system. A detailed process in this regard will be finalized by the MSI in consultation with the CHiPS.

6. An issue log shall be maintained by the MSI for the errors and bugs identified in the solution as well as any changes implemented in the solution. Issue log shall be submitted to the CHiPS on a monthly basis.

7. The MSI will inform the CHiPS, as per the agreed plan, about any new updates/upgrades available for all software components of the solution along with a detailed action report. In case of critical security patches/alerts, the MSI shall inform the CHiPS immediately along with any relevant recommendations. The report shall also contain the MSI's recommendations on update/upgrade, benefits, impact analysis etc. The MSI needs to execute updates/upgrades and update all documentations and Knowledge databases etc. The MSI will carry out all required updates/upgrades by following a defined process at no additional cost.

8. The MSI will be responsible for user and access management

3.5.1.2. Issue Identification and Resolution

Errors and bugs that persist for a long time, impact a wider range of users and are difficult to resolve in turn lead to application hindrances. The MSI shall resolve all the application problems through implementation of the identified solution (e.g. system malfunctions, performance problems and data corruption etc.). The monthly issue logs on problems identified and resolved would be submitted to the CHiPS along with recommended solutions.

3.5.1.3. Software Version Control

The MSI needs to follow all such processes (based on industry ITSM framework) at all times. For any change, MSI shall ensure:

- Detailed impact analysis is conducted
- All change plans are backed by roll back plans
- Appropriate communication on change required has taken place
- Requisite approvals have been received
- Schedules have been adjusted to minimize impact on the Production environment
- All associated documentation is updated post stabilization of the implemented change
- Version control is maintained for all software changes

The MSI shall define the version control process through version control process. For any changes to the solution, the MSI has to prepare detailed documentation including proposed changes and impact to the system in terms of functional outcomes/additional features added to

the system etc. The MSI shall ensure that software and hardware version control is carried out for the entire contract duration.

3.5.1.4. Release Management

The Release Management is used for the release of software of software, upgrades and patches. This ensures the availability of licensed, tested, and version-certified software, which will function as intended when introduced into the production environment. In the context of IPeG System, release management is required to be handled at two levels.

- Troubleshooting of Level-3 software incidents would result into modification or update of the existing IPeG software deployment in production environment. It will be responsibility of the MSI to obtain the modified software and carry out user acceptance test, if required, and then deploy in the product environment.
- The MSI is responsible for development and maintenance of support applications. Level-3 software incidents related to support application or other enhancements would require change in the respective modules. It will be responsibility of the MSI to test the modified software (including UAT, if required) and then deploy in the product environment.
- The overall release management and version control of the IPeG System will be the responsibility of MSI.
- The MSI shall carry out following activities in the release management process:
    - Plan releases as per the requirements for the approved changes
    - Build release packages for the deployment for approved changes (one /many) into QA/Staging /production
    - Design, test and implement procedures (mechanisms) for the distribution of approved changes to QA/Staging /production environment
    - Effectively communicate and manage expectations of the customer/internal stakeholders/end customer during the planning and rollout of new releases
    - Monitor, Control, and Report the distribution and installation of changes to all concerned stakeholders.
    - Deploy the release as per guidelines
- For the release, the following process may have to be defined:
    - Release Planning Process
    - Release Building Process
    - Release Testing Process
    - Release Deployment Planning Process
    - Release Deployment Process
    - Client Release Management Process
    - Hosting Release Management Process
- The MSI shall document the above processes and submit to the CHiPS for sign-off.

3.5.1.5. Maintain System Documentation

- The MSI shall maintain at least the following minimum documentation with respect to the IPeG system:
    - High level design of whole system

- Low level design for whole system/module design level
- Updated System Requirements Specifications (SRS)
- Any other explanatory notes about system
- Traceability matrix
- Compilation environment

- The MSI shall also ensure that any software system documentation is updated with regard to the following:
  - Source code is documented
  - Functional specifications are documented
  - Application documentation is updated to reflect on-going maintenance and enhancements including FRS and SRS in accordance with the defined standards
  - User manuals and training manuals are updated to reflect on-going changes/enhancements
  - Standard practices of version control and management are adopted and followed

3.5.1.6. Application Software Enhancements and Customization

For minor enhancements and customization in the IPeG components provided by MS, the business and technical services team of MSI will be utilized. For other enhancements and customization (including addition of components), the MSI will need to raise a change request. The CHiPS shall make payment to the MSI on the man-month rates submitted as part of the commercial bid.

3.5.1.7. Support during Audits

The CHiPS may get the system audited by 3rd party auditors including performance auditors, security auditors, etc. The MSI shall provide necessary support and co-operation for the audit and close the findings of the audit. The CHiPS may arrange for the ISO 27001 audit to be conducted for the IPeG System. The MSI shall cooperate, provide necessary support and close the findings of the audit.

3.5.2. Annual Technical Support (ATS)

The MSI shall be responsible for providing annual technical support for the COTS/OTS products supplied by respective OEMs during the entire maintenance and management phase. It is mandatory for the MSI to take enterprise level annual support over the entire contract duration, at minimum, for the software(s) as mentioned in the Bill of Material provided by the MSI.

3.5.3. Warranty and Operations

The MSI will be responsible for the following:

- Supply a comprehensive OEM warranty of IT infrastructure supplied under this engagement for the duration of the project after Go-Live.
- MSI will be required to provide Annual Technical Support (ATS) for System Software, COTS, OTS, Middleware, SDKs, etc. as supplied and commissioned under this engagement for a period of entire project duration from the Go-Live.
- MSI will be required to provide Annual Technical Support (ATS) for software as supplied and commissioned under this engagement for the contract duration.
- MSI needs to have OEM support for all the IT Hardware components with documentation which shall be submitted to CHiPS on annual basis.
- MSI will be responsible for coordinating with the OEM for the rectification of any problem covered under the comprehensive warranty. MSI will be responsible for resolution of any problem in IT hardware as per defined service levels.
- MSI will be required to maintain a log of Warranty and AMC status of each of the existing assets. For assets whose AMC/Warranty is due for expiry, intimation to CHiPS shall be provided at least 3 months prior to the expiry of the contract and MSI shall take action for renewal/extension of AMC/Warranty.

3.5.4. Solution Performance Management and Optimization

The MSI would be required to meticulously manage, monitor and optimize the performance of the components and troubleshoot any issues that may arise. The MSI is expected to make reports and provide monthly updates to the CHiPS. The MSI will be responsible to ensure the performance issues that may be arising through department's/third-party systems are resolved and will extend support to department, if required. The MSI must provide a full description of the services and processes that will be undertaken to implement the manage, monitor and optimize the performance in the most efficient, timely and comprehensive manner.

3.6. Call Centre Setup and Operations

3.6.1. Call Centre Setup

As part of the call centre setup, the MSI will be responsible to:

1. Provide, integrate and manage a dedicated toll-free number for the Call Centre and will bear the operational cost of this number. This number should be accessible free-of-charge to the resident from all the landline and mobile network operators in India.
2. Ensure availability of physical space for the call centre along with necessary Electrical (Power Supply, Wiring, Power Sockets, Lights, etc.) and Physical Infrastructure (Tables, Chairs, etc.).

3. Provide necessary IT (Hardware, Software, Network) and Non-IT Infrastructure (Communication Equipment such as EPBX, IVR, Dialler, Telephones, Headsets, etc.).
4. Commissioning, configuration, customization/implementation, integration, and maintenance of an enterprise level call centre software including Customer Relationship Management (CRM), IVRS, etc. solution
5. Integration of call centre software(s) with relevant IPeG components
6. Responsible to analyse and fulfil the requirements of IT infrastructure for hosting of the call centre software(s) to meet the availability, performance and response times required to meet the Call Center service levels
7. Prepare a detailed plan for setting up of Call Centre Operations with timelines and activities and submitting the same for CHiPS's approval
8. Prepare standard operating procedures of call centre including call handling processes, quality assurance and escalation management
9. Impart proper training in soft skills like call handling, exposure to related application etc. so as to prepare the customer service executives to attend/make to calls effectively. MSI shall also prepare the required training material and ensure recurring training of call centre agents on a periodic basis.
10. The MSI will be responsible for creation of FAQs for Call Centre. These FAQs shall contain the frequently asked questions as well as their optimal responses to the questions. The FAQs will have a detailed script on step-by-step questions that the agent would be required to ask the citizen and provide the required response.

The MSI will provide PRI lines and a dedicated number for the Call Centre and will bear the operational costs of these items. The MSI should ensure that the call centre has requisite IT and other Infrastructure to support the project requirements. MSI shall be required to provide and maintain all IT and Non-IT infrastructure for successful operations of the call centre including, but not limited to, the following:

a. Hardware such as desktop with headsets, telephones, etc.
b. Software such as call centre application, Computer Telephony Interface connector to integrate call centre application and IVR, Call barging and recording software, etc.
c. Communication Equipment such as IVR, Dialler, EPBX, etc.
d. Automatic Call Distributor (ACD) for distribution of incoming calls to Call Centre staff as they are received. MSI shall be responsible for installation of the ACD. ACD should have at least the following features:
    - System should be able to intelligently route the callers to Call Centre staff based on their availability to take calls on first come first serve basis.
    - Standard features like Call Transfer, Conference, Barge-in, Dialled Number Identification Sequence (DNIS), Automatic Number Identification (ANI), and Caller Line Identification (CLI) etc.

- System should announce the queue waiting time for the caller before getting attended by a Call Centre
- System shall support the ability to play customized announcements per queue as defined by the administration.

3.6.2. Call Centre Operations and Maintenance

The operations and maintenance of the Call Centre are defined in this section. The MSI will be responsible to adhere to all instructions provided below:

- MSI will also be required to maintain the infrastructure provided at the Call Centre for a period of entire contract.
- MSI shall be responsible for ensuring that the infrastructure provided by it is operational during operational hours of call centre.
- The CRM solution should be used to log all incidents and queries in the system for generating id and track the logged query
- MSI shall be responsible for operations, maintenance and support of CRM solution as part of the maintenance and technical support from OEM including associated updates and upgrades.
- MSI shall generate and provide CRM Reports on daily, weekly, monthly, quarterly and yearly basis.
- MSI shall also be responsible for analysis of the CRM reports to continuously identify improvements in the CRM operations
- MSI will extend all the required support to the CHiPS during their Random or Regular audits of the call centre operations and call centre facilities.
- MSI shall ensure proper procedures are established for Call Centre systems in the event of a disaster to protect and ensure continuation of Call Centre services.
- MSI will also be responsible for the optimization of the IVR. The call routing and management is expected to be optimized as per the trend of calls to the Call Centre.

3.6.2.1. Reporting

The reporting responsibilities of MSI are as follows:

a. MSI should generate standard reports to measure/verify various service level(s), to monitor the performance of agents, etc.

b. Call centre application should provide a detailed report including reports for measurement of compliance against SLA.

c. MSI shall prepare and submit reports to the CHiPS as per the mutually agreed reporting structure. These reports shall include but not limited to the following:

   - Incident, devices and system logs/ security logs (category, severity and status of call etc.)
   - Incidents escalated

- SLA compliance/non-compliance report
- Problem Management
- Key learning from similar previous experience
- Escalation procedure for handling significant issues
- Call Centre staffing

d. MSI and CHiPS will mutually agree on the format of the reports to be submitted by the MSI to CHiPS. MSI must provide at minimum the following reports:

- Reports based on time period
- Type of queries/demand/analysis
- Repeat request or complaints analysis
- Call waiting time
- Lost calls
- Call time (Average Talk Time/Hold Time/Handle Time)
- Hourly call details
- Requests pending for more than defined time period
- Calls Handled
- Abandoned Call Rate
- Delay Before Abandon (Average/Longest)
- Staffing related Report
- Other monthly MIS, SLA reports, number of agents logged in

3.6.2.2. Monitoring

The MSI should extend all the required support to CHiPS for monitoring and access all subsystems and records pertaining to call centre operations for the CHiPS. The MSI shall be responsible to assist the CHiPS in monitoring of the call centre agents and operations.

3.6.2.3. Key features of the Proposed Call Centre

The key features of the proposed Call Centre are enlisted in the table below:

No. of Seats	MSI needs to analyse and size accordingly to the requirement of IPeG project. The well-trained and well-equipped call centre agents and supervisors to be provided by MSI.
Duration	One month before go-live and to continue till end of project duration
Languages supported	Hindi, English, Chhattisgarhi

Operations	• All the days of the week (Monday – Sunday) • 10:00 to 19:00
Accessibility	Accessible through a Toll-Free Number, IVR Solution
Review	Quarterly review of call volumes and number of seats required to provide services through Project Management Unit
Location	Within the state of Chhattisgarh, in Raipur or Nava Raipur

3.7. Helpdesk Setup and Operations

3.7.1. Helpdesk Setup

The MSI would be responsible for helpdesk setup and operations.

- Provide, integrate and manage a dedicated number for the helpdesk and will bear the operational cost of this number.
- Provide necessary IT (Hardware, Software, Network) and Non-IT Infrastructure (Communication Equipment such as EPBX, IVR, Dialler, Telephones, Headsets, etc.).
- Commissioning, configuration, customization/implementation, integration, and maintenance of an enterprise level helpdesk software including ITSM, IVRS, etc. solution
- Integration of helpdesk software(s) with relevant IPeG components
- Responsible to analyse and fulfil the requirements of IT infrastructure for hosting of the helpdesk software(s) to meet the availability, performance and response times required to meet the helpdesk service levels
- MSI shall be responsible for setting up an IT helpdesk operation at state level for the Department officials to support IT issue resolution
- MSI shall prepare a detailed plan for implementation of IT Helpdesk in line with overall project timelines. This plan shall be prepared in coordination with the CHiPS.
- MSI shall be responsible to prepare standard operating procedures (SOP) for the IT helpdesk. The SOP should include detailed process flow for issue logging, issue prioritization guidelines, problem security codes and escalation procedures, issue resolution etc.
- SOP should also include predetermined restoration/resolution targets based upon Service Level Agreements defined as part of this RFP
- The IT Helpdesk will be used by the MSI, MSI staff, Department Officials, Field Official(s), etc.
- MSI shall deploy CRM software/ Incident Management module of EMS for the helpdesk which shall be accessible to all users through the IPeG portal for logging issues
- MSI would provide and implement a comprehensive IT Helpdesk which would be integrated with IPeG solution.
- The software license(s) of the Helpdesk application shall be in the name of the CHiPS
- IT Helpdesk application shall record all incidents as service requests
- The IT Helpdesk application would maintain complete incident history of all incidents recoded at the IT Helpdesk.

- IT Helpdesk application should provide workflow and hierarchy through which each incident should move based on Incident severity, classification and owner.
- IT Helpdesk application shall capture all the relevant information of incident logger, incident under consideration etc.

The MSI will be responsible for training to Helpdesk Manpower

- MSI should make arrangements for imparting proper training and soft skills, call handling, exposure to related application, required technical skills etc. so as to prepare the MSI's staff at the IT Helpdesk to answer and resolve issues/ incidents.
- The MSI shall include the cost of training the resources for any new process, modules, etc.
- MSI shall be responsible for periodic training of the staff at the IT helpdesk. A detailed training calendar should be prepared and submitted by the MSI to the CHiPS.

The MSI will be responsible for creation of FAQs for Helpdesk agents. These FAQs shall contain the frequently asked questions as well as their optimal responses to the questions. The FAQs will have the technical solution to be provided to the ticket raiser to troubleshoot their problems.

3.7.2. Helpdesk Operations and Maintenance

IT Helpdesk would have following major activities and tasks:

- Log incidents/issues as service requests and provide a unique service request number. Acknowledgement should be sent to user along with service ticket number through an email immediately on issue logging. All issues logged should be assigned a severity level (L1/L2 or L3). Indicative severity level definitions are given below:

Severity	Definition
L1	MSI will be required to train its staff to resolve the L1 issues by themselves and if required can escalate for L2 support team. L1 issues/ incidents are the ones which have a minimal business impact. These issues/ problems could have any of the following characteristics: • No impact on processing of normal business activities. • A low impact on the efficiency of users • Has a simple workaround • Enhancement requests
L2	MSI will be required to train the its staff at districts to resolve the L2 issues by themselves and if required can escalate for L3 support team, i.e. MSI. It could be required that some of the L2 issues are important in nature and thus MSI will be required to address them. L2 level problems are the ones which have a significant business impact. These problems could have any of the following characteristics: • The efficiency of users is being impacted

Severity	Definition
	• Has a viable workaround • Severely degraded performance (slow service)
L3	L3 level problems are the ones which have a critical business impact. The IT helpdesk will record such incidents and if required inform the MSI directly to address the issue at the earliest. L3 issues would be resolved by MSI. These problems could have any of the following characteristics: • Entire or part of any service unavailable (including APIs) • Incorrect behaviour of the system (wrong calculations, etc.) • Security Incidents • Data Theft/loss/corruption • Severe impact on customer satisfaction • No work-around to mitigate the disruption in service • Repeat calls (same problem that has occurred earlier reported more than 2 times)

Table 1: Level Definition

- IT Helpdesk staff should have a provision to increase the severity levels, if required.
- The Helpdesk staff shall have provisions through the application for coordinating with concerned vendor in case issues are pertaining to any external entity product/support like:
  - Respective OEM team
  - Cloud or SDC Support Team
  - Network Provider
  - Any Other
- MSI shall analyse all the incidents and provide a root cause analysis report on a periodic basis for all the recurring incidents. MSI shall ensure that resolution is provided for these problems by respective technical teams/vendors to prevent further issues due to the same cause. The report for the same should be submitted to CHiPS.
- Track and route incidents/service requests and to assist end users in answering questions and resolving problems. Assign severity level to each ticket as per the SOPs.
- Issues which cannot be resolved by the IT Helpdesk should be routed to the concerned team of the MSI for resolution
- Escalate the issues/complaints, if necessary, as per the escalation matrix.
- Notifying users with the problem status and resolution through the tickets over email or SMS or both.
- Each service request would have a unique service request number.
- It is the responsibility of the MSI to ensure quality of IT Helpdesk.

- All incidents should be recorded, these records shall be retained on hard-disk for 30 days for easy retrieval.
- Incidents which are not meeting SLAs and which are exceptional in nature (highly critical, wider spread, etc.) shall be escalated as per defined escalation matrix.
- IT Helpdesk should comply with SLAs applicable to them as mentioned in this RFP. Non-adherence to SLAs shall lead to imposition of penalty.
- Continuous Improvement: MSI shall ensure continuous improvement in the IT Helpdesk Operations. The MSI shall:
    - Prepare Knowledge base for frequently reported problems along with the resolution steps/solutions and publish on the portal.
    - On a quarterly basis, carry out the analysis of help desk tickets (open and closed) to identify the recurring incidents and conduct a root cause analysis on the same. MSI shall submit a report to CHiPS with the analysis and provide inputs to CHiPS on user training requirements, awareness messages to be posted on the portal, redesign recommendations and/or application enhancements (functional/design) based on help desk ticket analysis. The objective of the analysis should be to address the repeat incidents and enhance the delivery of services to the end users.
- MSI shall prepare and submit reports to CHiPS as per the mutually agreed reporting structure. These reports shall include but not limited to the following:
    - Incident logs (category, severity and status of call etc.)
    - Incidents escalated
    - SLA compliance/non-compliance report with reasons for non-compliance
    - Detailed analysis of the calls containing opportunities of automation, trainings, FAQs, etc.
    - IT Helpdesk the utilization reports, benchmarked against industry standards for similar application/environment.
- The MSI will also be responsible for the optimization of the IVR. The call routing and management is expected to be optimized as per the trend of calls to the Helpdesk.

The key features of the proposed Helpdesk are enlisted in the table below:

No. of Seats	MSI needs to analyse and size accordingly to the requirement of IPeG project, to begin with a 3-member team is envisaged. The well-trained and well-equipped call centre agents and supervisors to be provided by MSI.
Start	One month before go-live and to continue till end of project duration
Languages supported	Hindi, English, Chhattisgarhi
Operations	• All the days of the week (Monday – Sunday)

	• 08:00 to 24:00
Accessibility	Accessible through a Dedicated Number, IVR Solution
Review	Quarterly review of call volumes and number of seats required to provide services through Project Management Unit
Location	Within the state of Chhattisgarh, in the office of CHiPS within Raipur or Nava Raipur

3.8. Managed Cloud Hosting Services

MSI shall design an appropriate System Administration policy with precise definition of duties and adequate segregation of responsibilities and obtaining the approval for the same from CHiPS. Overall System Administration of the IT Infrastructure (Cloud Services) shall include following activities:

- Overall management and administration of infrastructure solution including servers, security components, network components, storage solution and others.
- MSI has to co-ordinate with other vendors, wherever required/applicable
- Performance tuning of the system as may be needed to enhance system's performance and comply with SLA requirements on a continuous basis.
- Security management including monitoring security and intrusions into the system to maintain the service levels as per SLA defined. Successful Bidder will strictly adhere to the Security Policy adopted by CHiPS
- Monitor and track cloud service performance and take corrective actions to optimize the performance on a weekly basis.
- Escalation and co-ordination with other vendors for problem resolution wherever required.
- Data storage management activities including regular backup, restore and archival activities.
- Support to system users with respect to attending to their requests for assistance in usage and management of the application.
- Whenever a component has to be replaced because of technical, functional, manufacturing or any other problem, it shall be replaced with a component of the same make and configuration.

3.8.1. Hosting Strategy for IPeG

The hosting strategy for the project is summarized below:

- **Aadhaar Authentication and Aadhaar Data Vault:** These components will be hosted in the State Data Centre by the MSI. The necessary hardware, software licenses, network, etc. will be provided by CHiPS.

- **IPeG Components provided by MSI (except Aadhaar Authentication and Aadhaar Data Vault):** These components will be hosted in the Cloud Hosting by the MSI. The necessary hardware, software licenses, network, etc. will be provided by MSI. After the end of 2nd year after go-live, the MSI will coordinate with the CHiPS to understand the readiness of State Data Centre 2.0 (hereafter referred to as SDC) and provide a detailed Bill of Material (current utilization and forecasted utilization) to CHiPS for decision. The concerned SI (SI-SDC) will coordinate with MSI to understand the requirements and submit a proposal to CHiPS for consideration. The CHiPS will take necessary decision on whether to continue on cloud provided by MSI or migrate to the SDC. In case CHiPS decides to migrate components to SDC, the MSI will support the SI-SDC in migration of the components from its own cloud to SDC. The MSI will continue to perform operations and management (except for cloud infrastructure).

3.8.2. General Requirements

1. The MSI should architect a Platform as a Service (PaaS) on Virtual Private Cloud (VPC) /Government Community Cloud (GCC) deployment model (as per MeitY) of a MEITY Empanelled Cloud Service Provider. In case of GCC model also, IPeG and infrastructure stack should be logically segregated from the other Government clients.

2. MSI shall assess the infrastructure requirements (including OS Instances, Storage, Networking, Security etc.) for hosting and maintaining all required applications/services. The MSI shall provide the services in conformance with the SLAs as described in the RFP.

3. The MSI should ensure that all peripherals, accessories, sub-components required for the functionality and completeness of the solution, including but not limited to devices, equipment, accessories, software, licenses, tools, etc. should also be provisioned according to the requirements of the solution.

4. CHiPS will not be responsible if the MSI has not provisioned some components, sub-components, assemblies, and sub-assemblies as part of bill of material in the bid. The MSI will have to provision the same to meet the solution requirements at no additional cost and time implications to CHiPS.

5. The Virtual Private Cloud services of the CSP should be available on pay as per usage model and Fixed-Billing model and should be sized by MSI basis the Guiding principles of IT infrastructure design section (On-Demand vs Fixed Billing). However, from CHiPS perspective, the billing would be done quarterly irrespective of Fixed/On-Demand model with the Cloud Service Provider.

6. The MSI should use Open Source Solution (Enterprise Edition) or COTS (Commercial-off-the-Shelf) license, for any application software that MSI would be deploying on VPC/GCC of CSP. Any purchase of license or support should be in the name of CHiPS or its nominated government agency.

7. The CSP should specify DC and DR locations. CHiPS may, at any point of time, require audit of the provisioned DC / DR environment; MSI/CSP is required to facilitate such timely audits.
8. The relational database system should be constructed in high availability mode with synchronous replication.
9. The MSI should decide basis the RTOs and RPOs and the SLAs the number of sites the application would be hosted on.
10. IPeG Solution and Cloud Services should be accessible via IPSec over internet to MSI operations team and MPLS/P2P leased line from the CHiPS network.
11. Any access that has active control has to be through dedicated network only.
12. DC and DR should be provided by the same CSP.
13. The solution should have ability to automatically provision services via a Web Portal (Self-Provisioning), provide metering and billing to provide service assurance for maintenance & operations activities. Detailed user level or user group level auditing, monitoring, metering, accounting, quota and show-back information is essential for the virtual private cloud platform to be offered.
14. MSI, in alliance with the CSP, should ensure seamless migration in case the underlying architecture is upgraded
15. The Virtual Private Cloud Services/Government Community Cloud Services of CSP should provide data migration services (both egress and ingress)
16. It is expected that the MSI will provide an integrated solution, after due consideration to the compatibility issues between various components. If there is a problem with compatibility between components, the MSI should replace the components with an equivalent or better component (that is acceptable to CHiPS) at no additional cost to CHiPS and without any project delays.
17. The Virtual Private Cloud Services of CSP should support and provision REST based API for each of the services for automation along with SDKs for platforms like Microsoft .net, Java/JavaScript, Python, PHP or Ruby. The MSI should be able to utilize these API's to set up routine jobs such as backup on an automated schedule wherever necessary.
18. The Virtual Private Cloud Services of CSP should also provide API Gateway services to create, host, monitor API services that may be required as part of the solution.

3.8.3. Policy Requirements

1. The MSI/CSP should confirm that data will reside in India and should not be accessed by any entity outside the control of CHiPS.
2. The “IPeG Data” and “Virtual Private Cloud Services/Government Community Cloud Services of CSP Infrastructure” must be maintained ONLY at the declared hosting site of CSP which should be communicated as part of the solution document.

3. The CSP shall not delete any data at the end of the agreement (for a maximum of 90 days beyond the expiry of the Agreement) without the express approval of the CHiPS.

3.8.4. Logical Partitions

1. All the applications would follow a three-tier architecture with clear separation of database tier/layer from application and web layers. For micro-services-based architecture, MSI should deploy Presentation, Logic and Database category of micro services on different VM's/Containers
2. The Web layer for applications accessed via Internet/MPLS shall be hosted in the DMZ zone/Subnet; the application layer should be hosted in the Militarized Zone or a separate subnet ensuring full security
3. The Database nodes (RDBMS) should be in a separate zone with higher security.
4. All management servers which are not directly accessible through the internet will be kept in Management Zone. Active directory, Different modules of Enterprise Management Servers (including network, server, database, helpdesk etc.), Single-Sign-On, access and identity management server, Security Operations Centre, etc., will be a part of this management layer.
5. There will be separate VLANs/Subnets created for various environment as per RFP to segregate development and testing traffics from the production. Appropriate firewall policies/rules shall be implemented to have further security between different zones.
6. For the purpose of sizing, the MSI would size the solution on various environments listed in Tender document – Scope of work.

3.8.5. Configuration

1. Cloud service should support the needs of I/O-intensive workloads, particularly database workloads that are sensitive to storage performance and consistency in random access I/O throughput and hence once provisioned it should be possible to configure the IOs
2. The CSP should offer a service to quickly deploy and manage applications in the cloud by automatically handling the deployment, from capacity provisioning, load balancing, auto-scaling to application health monitoring.
3. The MSI shall ensure that identity solution is utilized and use best practices like least privilege, changing of passwords regularly, enable Multi Factor Authentication for Privileged user or for Secure Delete are utilized.
4. Cloud service should support parameterization for specific configuration.

3.8.6. Services

1. The CSP should own and offer services like Database as a service, DNS, Data warehouse Analytics, Message queuing; such services is preferred to be managed from a single console.

2. The MSI/CSP should offer support at any time, 24 hours a day, 7 days a week, and 365 days per year via phone, chat, and email.
3. The CSP should provide a web interface with support for multi-factor authentication to access and manage the resources deployed in cloud.
4. Able to define guidelines for provisioning and configuring cloud resources and then continuously monitor compliance with those guidelines.
5. Provide Audit logs of the account activity to enable security analysis, resource change tracking, and compliance auditing.
6. Provide data migration services either with the help of a Cloud Native or SaaS/Third Party Software Deployed on VM solution for moving data of all types and sizes into and out of cloud.

3.8.7. Compute

1. The system must be Scalable, Reliable, Highly Available & should provision to upgrade/downgrade virtual machine configuration (vCPU, vRAM, storage) parameters seamlessly based on demand with zero downtime.
2. The PaaS service should have the ability to Auto-Scale (Horizontal) on demand. The service should support automatically launching or terminating instances based on parameters such as CPU utilization or other factors basis the demand. The solution should also be able to do continuous monitoring and optimization of auto-scaling rules and limits. The Cloud service should have self-service provisioning where there is zero dependency on CSP and MSI should be able to provision the service in an agile manner without any intervention from CSP.
3. Cloud service must offer self-service provisioning of multiple instances concurrently either through a programmatic interface (API/CLI) or through a management console.
4. The MSI shall ensure that the database layer for the applications in production shall be deployed in N+N High availability mode. The Web and Application layer for the applications in production shall be deployed in N+1 high availability mode (Active-Active). However, the choice of Active-Active at Application layer is upon the MSI.
5. The MSI shall ensure that the services that are deployed on partitions/virtual images and are required in cluster and/or load-balancing mode, shall be deployed in such a manner that the load sharing/failover is across the OS instances and NOT amongst partitions of the same OS instance. In case of a hardware or software component failure in one partition, other partitions must not be shut down or rebooted.
6. Please remark on the core: vCPU ratio that would be used while giving out the VMs
7. Please confirm that for production instances no burstable vCPU /shared vCPU would be used

3.8.8. Networking

1. Cloud service should entail use of Virtual Private cloud which would ensure logical isolation of the infrastructure.
2. Cloud service should be able to support multiple (primary and additional) network interfaces. Cloud service should be able to support multiple IP addresses per instance.
3. Cloud service/MSI should support the ability to create a network interface, attach it to an instance, detach it from an instance, and attach it to another instance.
4. There should be redundancy from two different service provider for the MPLS line/P2P leased line
5. Cloud service should support capabilities such as single root I/O virtualization for the isolation of PCI Express resources for manageability and higher performance.
6. Cloud service should be able to support IP address ranges specified in RFC 1918 as well as publicly routable CIDR blocks.
7. The CSP must support IP addresses associated with a customer account, not a particular instance. The IP address should remain associated with the account until released explicitly.
8. Cloud service should support a Hardware/Software based VPN connection over MPLS/P2P leased line from the cloud DC/DR to site-site VPN (IPSec) over Internet for MSI sites for Operations Management
9. Cloud service should support connecting two virtual networks to route traffic between them using private IP addresses.
10. Cloud service should support Load balancing (both local and Global) of instances across multiple host servers.
11. Cloud service should support multiple routing mechanism including round-robin, failover, sticky session etc.
12. Cloud service should support a front-end load balancer that takes requests from clients over the Internet and distributes them across the instances that are registered with the load balancer.
13. Cloud service should support an internal load balancer that routes traffic to instances within private subnets.
14. The CSP should be able to provide a 10Gbps network connectivity between the servers if required.
15. The internet bandwidth shall be clean with DDOS protection and active monitoring to be provided by the ISP or by the CSP.
16. The Virtual Private Cloud /Government Community Cloud Services of CSP should have the following service available

- IPv4,IPv6
- DHCP
- IPSec VPN Tunnel Creation
- SSL VPN
- DNS services
- Load Balancer (Balancing between multiple sites)
- L4 and L7 Load Balancer
- At least L3,4,6,7 Anti-DDoS solution

3.8.9. Storage

3.8.9.1. Block

1. The CSP shall be capable to block storage volumes greater than 500 GB/ 1 TB in size.
2. Cloud compute service should support local storage for transient block storage requirements.
3. Cloud service should support Solid State Drive (SSD) backed storage media that offer single digit millisecond latencies. There should be an option to choose the media type with respect to the type of environment. All production instances storage should be SSD backed with minimal latencies. Other environments need not be on SSD.
4. Data at Rest and Data in transit should be encrypted with customer owned keys provided by CSP. Ciphers should be at least 256-bit Advanced Encryption Standard (AES-256).

3.8.9.2. Object

1. The CSP should offer secure, durable, highly scalable object storage for storing and retrieving any amount of data on demand.
2. The CSP should support an extremely low-cost storage service that provides durable storage with security features for data archiving and backup.
3. Data at Rest and Data in transit should be encrypted with customer owned keys provided by CSP. Ciphers should be at least 256-bit Advanced Encryption Standard (AES-256).
4. Cloud Service should support lifecycle management configuration
5. The place where the objects would be stored should be configurable and all objects should stay in India.
6. Cloud service should be able to send notifications when certain events happen at the object level (addition/deletion).

Cloud service should be able to provide audit logs on object storage buckets/ container which should include details about access request and error code.

3.8.9.3. File Storage

1. The CSP should offer a simple scalable file storage service to use with compute instances in the cloud.
2. Cloud service should support petabyte-scale file systems and allow thousands of concurrent NFS/SMB connections.
3. Cloud service should support scalable IOPS and throughput performance at any scale.
4. Data at Rest and Data in transit should be encrypted with customer owned keys provided by CSP. Ciphers should be at least 256-bit Advanced Encryption Standard (AES-256).

3.8.10. Backup

1. The CSP should offer a service with ability to take regular and scheduled backup.
2. The MSI should propose cloud native solution or use a SaaS based/Third Party Software deployed on VM based backup software.
3. Low cost Object Storage should be utilized as the backup target. If there is need to use the block-based storage for backup target for staging or as a whole, the same should be flagged and explained.
4. The MSI/CSP should configure, schedule and manage backups of all the data including but not limited to files, folders, images, system state, databases and enterprise applications
    - An Initial Full Backup
    - Daily Incremental with 15 days retention
    - Weekly full with 30 days retention
    - Monthly Full with 30 days retention on Object Storage and 12 months retention on Long Term storage
    - Yearly Full with 30 days retention on Object storage and 7 Years retention on Long term storage
    - For the databases, perform a twice weekly full database backup, with a three times daily backup of database log files
    - Encryption of all backup files and data and management of encryption keys as a service that can be enabled for IPeG that require such a service.
    - Different Tiers of Backup storage should be chosen depending upon the reads/restore that would be required

- Restoration Policies:
  - Backups taken in last 2 months: Once in a month
  - Backups taken in last 6 months: Once in a Quarter
  - Backups taken in last 1 Year: Once in Half Year
  - The restoration would be performed on a random basis and would be done against a ticket logged in the ITSM tool.

S. No	Backup Type	Backup Frequency	Retention Period	
			Object Storage	Long Term Storage
1	Daily Backup	Daily Incremental	15 days	Not Required
2	Weekly Backups	Weekly Full	30 days	Not Required
3	Monthly Backup	Monthly Full	30 days	12 months
4	Yearly Backup	Yearly Full	30 days	7 years

5. Any data requested from Long Term Storage should be retrievable within a time span of 12 hours.
6. The Long-Term Storage should have an option of enforcing WORM (Write Once, Read Many) policy for section of data that requires the same.
7. Data at Rest and Data in transit should be encrypted with customer owned keys. Ciphers should be at least 256-bit Advanced Encryption Standard (AES-256).

3.8.11. Disaster Recovery

1. The solution should be architected to run on cloud services offered from multiple data centre facilities to provide business continuity with no interruptions in case of any disruptions/disaster to one of the data centre facilities. In case of failure, automated processes should move customer data traffic away from the affected area. The Cloud Service Provider should provide adequate bandwidth between the Data Centre Facilities to provide business continuity.
2. DR should be available at time of disaster at DC. MSI should size solution as per defined RPO and RTO in the RFP.
3. In the event of a Primary site failover or switchover, DR site should take over the active role, and all requests should be routed through that site.

4. MSI/ CSP should offer switchover and switchback of individual applications (from services standpoint) apart from the entire system

5. In case of failover to DR site (once disaster is declared) within the defined RTO, the SLA would not be applicable for RTO period only. Post the RTO period, SLA would start to apply and should be measured accordingly.

6. In case of disaster at DC site (within the defined RTOs and RPOs), the DR should be available (with its data) on-demand basis, wherein 100% of the services of DC (Production environment) would run from DR site (after the RTO time and with the RPO level). Once the DC is restored, failback to DC is to happen.

7. DR should be provisioned with 100% capacity as provisioned in the DC. System Architecture to be designed to achieve Near Zero RPO and 2 Hours RTO.

3.8.12. Security Guidelines and Requirements

1. The MSI shall be responsible for ensuring security of IPeG applications and infrastructure from any threats and vulnerabilities. The MSI shall address ongoing needs of security management including, but not limited to, monitoring of various devices / tools such as firewall, intrusion prevention/ detection, content filtering and blocking, virus protection, even logging & correlation and vulnerability protection through implementation of proper patches and rules. For detailed, please refer to RFP Volume-II.

2. The Virtual Private Cloud Services of the CSP shall be fully secure with no scope of data breach/leaks/thefts/data mining/privacy breach etc. It would be MSI responsibility that for the layers where MSI is managing (For example in IaaS, above Hypervisor) all the relevant security layers are deployed. MSI should also ensure that CSP is also fulfilling all its responsibility (For example, in IaaS, Hypervisor and below, Physical, Network, Perimeter etc.). Please refer to PaaS section in Guiding Principles for delineation of responsibilities with respect to PaaS.

3. The MSI shall be responsible for ensuring security of IPeG application and infrastructure from any threats and vulnerabilities. The MSI shall address ongoing needs of security management including, but not limited to, monitoring of various devices / tools such as firewall, intrusion prevention/ detection, content filtering and blocking, virus protection, even logging & correlation and vulnerability protection through implementation of proper patches and rules.

4. The CSP should offer fine-grained access controls including, conditions like time of the day, originating IP address, use of SSL certificates, or authentication with a multi-factor authentication device.

5. Cloud service should offer a secure way to login (like public and private keys) and should have audit details which should tell about the keys last use details support reporting a user’s access keys last use details.

6. Cloud service should provide a mechanism to test the effects of access control policies that are attached to users, groups, and roles before committing the policies into production.

7. Cloud service should support a policy validator to automatically examine non-compliant access control policies.
8. Cloud service should support features such as user and group management.
9. Cloud service should allow users to reset their password in a self-service manner.
10. The CSP should offer a service to create and control the encryption keys used to encrypt user data.
11. Cloud service should support encryption of data on volumes, disk I/O, and snapshots using industry standard AES-256 or equivalent cryptographic algorithm. Data at Rest and Data in transit should be encrypted with customer owned keys. Ciphers should be at least 256-bit Advanced Encryption Standard (AES-256).
12. Cloud service should support auditing with features such as what request was made, the source IP address from which the request was made, who made the request, when it was made, and so on.
13. Cloud Service should also provide for Database Activity Monitoring
14. The MSI shall be responsible for ensuring security of IPeG application and infrastructure from any threats and vulnerabilities. The MSI shall provision and monitor the following security components/services (please also refer to Section 3.9.4)
    - Layer 4 Firewall
    - Layer 7 Firewall (WAF)
    - Intrusion prevention/ detection(Network and Host level)
    - Content filtering and blocking
    - Virus protection
    - Event logging & correlation
    - Vulnerability protection through implementation of proper patches and rules.
    - Vulnerability Assessment and Penetration testing before go-live of any module
    - Database Activity Monitoring
    - 2 Factor Authentication
    - Web Gateway with Content Filtering and Proxy Solution
    - Anti-Advanced Persistent Threat
    - Anti-DDoS
    - Anti-Virus
    - Data Leakage Prevention

- SSL VPN
- Email Gateway
- Privilege Identity Management

3.8.13. Data Security & Information Lifecycle Management

1. Policies and procedures shall be established for the labelling, handling, and security of data and objects which contain data. Mechanisms for label inheritance shall be implemented for objects that act as aggregate containers for data.
2. Policies and procedures shall be established with supporting business processes and technical measures implemented for the secure disposal and complete removal of data from all storage media, ensuring data is not recoverable by any computer forensic means.
3. Multi-tenant organizationally owned or managed (physical and virtual) applications, and infrastructure system and network components, shall be designed, developed, deployed, and configured such that provider and customer (tenant) user access is appropriately segmented from other tenant users, based on the following considerations:
    - Established policies and procedures
    - Isolation of business-critical assets and/or sensitive user data, and sessions that mandate stronger internal controls and high levels of assurance
    - Compliance with legal, statutory, and regulatory compliance obligations

3.8.14. Identity and Access Management

1. The Virtual Private Cloud/Government Community Cloud Services of CSP should provide Identity and Access Management service for the layer managed by CSP and MSI should bring in identity and access management solution (3rd Party or Cloud Native) for the layer that would be managed by them (For example, for the layers Data and above in case of PaaS, MSI should bring in respective tools). The solution should ensure that features like Multi-factor Authentication (Physical token based or Virtual Token Based), enforceable password policies, defining of roles both for resources and users, federation capabilities with other 3rd party Directory Services are present.
2. User access policies and procedures shall be established, and supporting business processes and technical measures implemented, for ensuring appropriate identity, entitlement, and access management for users with access to data and organizationally-owned or managed (physical and virtual) application interfaces and infrastructure network and systems components.
3. Policies and procedures shall be established to store and manage identity information about every person who accesses IT infrastructure and to determine their level of access. Policies shall also be developed to control access to network resources based on user identity.

3.8.15. Governance & Risk Assessment

1. The MSI/CSP should have organizational practices in place for policies, procedures and standards for application development and service provisioning as well as design, implementation, testing, use, and monitoring of deployed or engaged services in the cloud.
2. Audit plans shall be developed and maintained to address business process disruptions. Auditing plans shall focus on reviewing the effectiveness of the implementation of security operations. All audit activities must be agreed upon prior to executing any audits.
3. Risk assessment results shall include updates to security policies, procedures, standards, and controls to ensure that they remain relevant and effective
4. Solution shall have an audit and compliance feature which enables the Client agency to monitor the provisioned resources, performance, resource utilization, and security compliance. It shall have the following functionalities:
    - The solution should have automated security assessment service that should provide the following: (a). vulnerabilities assessment services, (b). Penetration Testing services, and (c). deviations from best practices such as password policy, unnecessary opened firewall ports, storage access policy, suggestion of data to archive
    - The system should have ability to set up alarms basis resource usage and the ability to define actions on triggering of those alarms (For example, ability to send an email when storage utilization has crossed x% or archive a storage section depending upon data type when it has crossed x% utilization)
    - Visibility into the performance and availability of the cloud services being used, as well as alerts that are automatically triggered by changes in the health of those services.
    - The solution should provide a dashboard that would list the details of any planned maintenance scheduled as well as any unplanned downtime faced in the recent past(past 3 months at least).
    - MSI/ CSP should provide dashboard for monitoring RPO and RTO of each application and database. The Dashboard should clearly show data replication process and any lag/ failure in data replication that should be notified through alerts to respective authorities.
    - The solution should be able to log all account and resource access into the account and resources (which might be resources logging into the account using API call or root/admin users or other users logging into the account).
    - The solution should be able to discover all provisioned resources in the Virtual Private Cloud Services/Government Community Cloud of the CSP and provide

details such as configuration items inventory, history of changes to such configuration items, snapshot of resource inventory at a single point in past, set-up of policies to track provision of resources within a client defined rulesets and auto -notifications each time a configuration changes

- The solution should be able to suggest best practices to optimize overall cost of resources.

3.8.16. Compliance

1. The MSI/CSP should understand and incorporate the different types of laws and regulations that impose security and privacy obligations on the organization. Especially those pertaining to data location, privacy and security controls, records management and electronic discovery requirements.
2. The MSI/CSP should ensure that independent reviews and assessments are conducted at least annually to ensure that the organization addresses nonconformities with the established policies, standards, procedures, and compliance obligations.
3. The CSP should comply with international security standards like ISO27001, ISO 27017, ISO 27018, etc.

3.8.17. Business Continuity Planning

1. MSI shall define and submit (as part of the solution), a detailed approach for “Business Continuity Planning”; this should clearly delineate the roles and responsibilities of different teams during DR Drills or actual disaster; further, it should define the parameters at which “disaster” would be declared.
2. The CSP should have a practicing framework for business continuity planning and the plan development for which has been established, documented, and adopted to ensure all business continuity plans are consistent in addressing priorities for testing, maintenance, and information security requirements.
3. The CSP should practice Business continuity and security incident testing at planned intervals or upon significant organizational or environmental changes.
4. Incident response plans should be developed by the CSP which should involve impacted customers (tenant) and other business relationships that represent critical intra-supply chain business process dependencies.

3.8.18. Monitoring Solution

1. CHiPS intends to monitor operational activities to have a holistic view of the provisioned cloud services and their configurations to ascertain required features have been appropriately implemented. In this view, the MSI shall provision monitoring tools (third party or cloud native) for measuring the service levels and application/server/storage/network performance & utilization. Basis the inputs of

Monitoring Solution, the cloud services should be configurable with auto-change in provisioned resources as per the monitoring inputs.

2. The monitoring tool should publish (on portal) real-time status (of all the services) that is refreshed with at least 5 min frequency; further, the tool should publish all historical parameters for a period of minimum 3 months. The tool shall be capable of generating per day/month/quarter utilization reports

3. The Monitoring System should have the following components:

    - **Cloud Dashboards**: Collect and track metrics, collect and monitor log files, and set alarms to gain system-wide visibility into resource utilization, application performance, and operational health. Overall, monitoring platform should provide End to End monitoring of complete IT Infrastructure

        - **Server Monitoring**: Should monitor heterogeneous operating systems for both dedicated & virtual instances on CSP OS layer including (but not limited to) Windows 32/64 bit, all major flavours of Linux, etc.

        - **Application Monitoring**: To perform infrastructure aware application triage, i.e. pin point network issues causing application degradation.

        - **Database Monitoring**: Monitor multiple database servers and versions being proposed on each server

        - **Storage Monitoring**: Monitor IOPS, Latency etc.

        - **Network Monitoring**: Should provide capability to monitor any device based on SNMP v1, v2c & 3

        - **SLA Monitoring**: Support Service Level Agreements, Lifecycle Management including Version Control, Status Control and Audit Trail

    - **Audit Trail**: Provide logs of all user activity. The recorded information should include (but not limited to) identity/source IP of API caller, time of API call, the request parameters, and the response elements.

    - **Security Compliance**: Monitors cloud resources and provides alerts in regards to security gaps such as overly permissive access to certain ports, minimal use of role segregation using IAM, and weak password policies.

    - **Configuration Management**: Discovery of configuration items and their relationships and generate detailed, predefined custom report of configuration items and their configuration

    - **Systems Manager**: Provides a unified user interface to view operational data and automate operational tasks across cloud resources.

    - **Personal Health Dashboard**: Provides a personalized view into the performance and availability of the services customers are using, as well as alerts that are automatically triggered by changes in the health of those services.

- **End User Experience Monitoring**: To measure end users' experiences based on transactions without the need to install agents on user desktops.
- **Asset Management**: To keep track of license life cycle from procurement to disposal and auto discovery and management of software inventory deployed on network.

4. Dashboard for views for all the above monitoring layers and can provide proactive notifications and alerts on actions that should be taken to prevent a failure
5. The department may insist on the following regular reporting during the contract:
    - Availability of the cloud services being used
    - Summary of event-based alerts, providing proactive notifications of scheduled activities, such as any changes to the infrastructure powering the cloud resources
    - Reports providing system-wide visibility into resource utilization, application performance, and operational health through proactive monitoring (collect and track metrics, collect and monitor log files, and set alarms) of the cloud resources
    - Auto-scaling rules and limits
    - Report of all of the provisioned resources and view the configuration of each.
    - Summary of notifications, triggered each time a configuration changes
    - Incident Analysis in case of any un-authorized configuration changes.
    - Summary of alerts with respect to security configuration gaps such as overly permissive access to certain compute instance ports and storage buckets, minimal use of role segregation using identity and access management (IAM), and weak password policies
    - Summary of security assessment report that identifies the possible improvements (prioritized by the severity) to the security and compliance of applications deployed on cloud
    - Report on upcoming planned changes to provisioning, either possible optimizations, if any, indicating how the underutilized services can be reduced to optimize the overall spend, or required enhancements (e.g., upgrade to additional storage) to meet the service levels defined in the RFP.
6. The User / Admin Portal (User Profile Management, Trouble Management) should also be part of the solution.

3.9. Information Security

3.9.1. Process and Procedures

Some of the indicative and non-exhaustive security processes and procedures that shall be developed, documented, implemented, and maintained by System Integrator are listed and described below:

(i) **Process for security of data sources**: MSI shall develop processes to secure the data sources, which contains information that IPeG intends to store and retain. These data sources consists of various records contained in the IPeG components. Since this repository contains information that is of paramount importance to identify a resident and establish details about an individual, it needs to be protected at every stage of its lifecycle.

(ii) **Key management process**: MSI shall develop processes for securing cryptographic keys in IPeG ecosystem. HSM shall be used for effective key management and HSM management process shall be developed.

(iii) **Logging and auditing process**: Logs provide useful information to support troubleshooting, forensics, audits, trend analysis, internal investigations, incident response, and optimizing system and network performance. It is essential that IPeG collects, periodically reviews, and securely archives the security log data for a defined period of time. MSI shall develop logging and auditing processes ensuring security and retention of security logs.

(iv) **Process for use of portable media**: MSI shall develop and implement processes for use of portable media in CHiPS (incl. Call Centre, Helpdesk, State Data Center & Disaster Recovery Sites) premises such as USB drives, CDs, magnetic tapes, mobile devices, etc.

(v) **IT asset certification process**: MSI shall review, enhance, and implement of necessary security guidelines and measures before introduction or deployment of an IT asset in IPeG environment. System Integrator shall also evaluate and minimize impact to other existing processes, applications, devices, etc. affected by introduction of the new asset.

(vi) **Risk assessment and treatment process**: MSI shall develop and implement processes for identification, estimation, assessment, and treatment of security risks as well as Fraud detection in IPeG's applications, systems, office and Hosting (Cloud and DC/DR) locations, etc. basis IPeG's risk management framework.

3.9.2. Minimum Baseline Security Standards (or referred as Hardening standards)

(i) MSI shall be responsible for development, documentation, implementation, and maintenance of minimum baseline security standards for all provisioned IT infrastructure, such as OS, network devices, security devices, application platforms, databases, etc.

(ii) MSI shall develop, implement, and maintain version-wise hardening standards for all IT infrastructure while referencing CIS benchmarking or vendor specifications for hardening. All minimum baseline security standards shall be prepared in consultation with CHiPS.

3.9.3. Security Design Considerations

3.9.3.1. Security Architecture Principles

Architecture Principle	Description
Data Loss Prevention	Make sure that no end user sends sensitive or critical information outside the government network to unauthorized recipient.
Data Privacy and Confidentiality	Information is shared on a Need-To-Know basis and is collected/accessed/ modified only by authorized personnel.
Secure by Design	Security must be built into all stages and all aspects of architecture development. Security concerns extend to all the IT activities of the enterprise.
Key Management	Secularly managing encryption keys for IPeG platform would be implemented using hardware security module (HSM), which is already procured by CHiPS.

3.9.3.2. End-Point Security Architecture Principles

Architecture Principle	Description
Desktop level firewall	Protect the integrity of the system from malicious software code, filter inbound and outbound traffic, and alerting the user to attempted intrusions. Should be enabled on every desktop in network.
Intrusion detection system/Intrusion prevention system (IDS/IPS)	IDS/IPS should be implemented to monitors systems and identify malicious activity or policy violations while an IPS watches network traffic as the packets flow through it and identify suspicious activity, log information, attempt to block the activity, and then finally to report it.
Anti-virus and anti-malware	Every end point should have latest and updated version of suitable anti-virus and anti-malware installed. It detects and destroy computer viruses, malware and other malicious software code.
Compliance with Government Desktop Core	Servers and Desktops in the network should comply to list of security settings recommended by GDCC.

Architecture Principle	Description
Configuration (GDCC)	
Patch management	Security patches of various software should be regularly updated.
Data Loss Prevention	DLP make sure that end users do not send sensitive or critical information outside the business network. It also describes software / hardware products that help a network administrator control what data end users can transfer

3.9.3.3. Security Design Principles

Design Principle	Description
Data Minimization	Data minimization refers to the principle which requires personal data collected to be adequate, relevant, and not excessive in relation to what is needed for the purpose of processing. It is expected that effective data management and data governance would inherently pave way for incorporating data minimization in practice within IPeG. Building data minimization practices at different points in the data lifecycle will help IPeG to implement and demonstrate good data handling practices in line with regulatory and resident expectations.
Data Anonymization and Pseudonymization	Anonymization is a technique applied to personal data in order to achieve irreversible de-identification. It turns the data into a form which does not identify individuals and where identification is not likely to take place. True anonymization allows for a much wider use of the information. Anonymization allows more security as it prevents identification of individuals occurring. Even if an anonymized dataset is disclosed, the data will be devoid of any personal information. Anonymizing can be used on such specific datasets in IPeG, where the purpose or processing can be achieved even after anonymizing the data. This will be useful for use-cases of reporting, open data, policy planning, research and development etc. Pseudonymization is defined as the processing of personal data in such a way that the data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organizational measures to ensure that the personal data are not attributed to an identified or identifiable natural person
IPeG Data Sharing Protocols	To achieve the objectives of the IPeG Program, there is a need for enabling streamlined exchange of data between the Department(s)/Government Organizations. However, the data envisioned

Design Principle	Description
	to be exchanged between the Department(s)/Government Organizations may also be personally identifiable information or may be of a sensitive nature and may have certain restrictions under the law and applicable regulations with regards to sharing of such data. Furthermore, since the unregulated sharing of data may be the cause of several vulnerabilities to residents of the State of Chhattisgarh, including but not limited to the violation of the right to privacy of residents, the sharing of Data between various Department(s)/Government Organizations needs to be done in a controlled and streamlined manner and in compliance with applicable laws. IPeG has its own Data Exchange Framework and Guidelines which needs to be taken into consideration by MSI.
Secure access to IPeG Data Exchange Platform	The IPeG is a complex system in which many competing requirements from diverse stakeholders must be balanced. Security and privacy of personal data has to be fundamental in design as the system is collecting, storing, processing and/ or transferring large volumes of data related to the personal data of the residents. When creating a system of this magnitude, it is imperative that privacy and security of personal data becomes a key design consideration. Hence, an effective and efficient security infrastructure needs to be utilized.
Security by Design	The information security policies shall lay the foundation for establishing, implementing, maintaining, and continually improving the information security management system of the IPeG solution
Privacy by Design	The principles of privacy should be embedded in the design and there should not allow any discretion or authority to overrule the privacy provisions.
Data Integrity	Data integrity ensures data is correct, consistent and un-tampered. To ensure data integrity encryption must be used to deter malicious or negligent parties from accessing sensitive IPeG Platform data. For one to one sharing and smaller data sets symmetric key based data encryption should be used. This uses one key to both encode and decode the information. For all other purposes, asymmetric key based data encryption should be used with linked keys – one private and one public.
Federated databased with one-way linkage	While the IPeG will have a large repository of identity data stored in the social registry, one must resist the temptation to add all residents' attributes to it. Each department, integrated with the IPeG platform that uses the social registry may also have attributes that are important to their individual departments (for instance, the PDS requires information about income level, as well as family relationships), which may not be required by all systems. Since IPeG has adopted the strategy of storing the minimal amount of identity data, that is required for its purpose, and in particular has chosen to stay away from maintaining transaction data. In this

Design Principle	Description
	federated model, defined rules, protocols and processes are required to protect collation of data across the entire IPeG platform based on the privacy protection laws. It is expected that such a federated approach would result in service delivery system which is stronger, secure, scalable and more reliable than a single centralized approach. It is also important that the various departments that may have reference to the IPeG, but the IPeG does not maintain a reverse links to any of these department's systems.
Separation of duties and least privilege	Every department and every user of the IPeG solution should operate using the least set of privileges necessary to complete the task. This will limit the damage that can result from an accident or error, as well as reduce the number of potential interactions among privileged users/processes to the minimum. It is also recommended that more than one person should be required for the completion of a task, through spreading the tasks and privileges among multiple personnel. For a protection mechanism that requires two keys to unlock it is more robust and flexible than one that allows access to the presenter of only a single key, ensuring that no single accident, or breach of trust is sufficient to compromise the protected information. For example, each critical process such as shall have defined maker checker principle in place
DevSecOps model and Application configuration management	Security in IPeG solution will be a part of the design, implementation and operations process. Secure software development lifecycle aims to bring in security by design of the IPeG platform. Security assessment and controls will be implemented at various stages of the software development lifecycle to embed security features right into the development process

3.9.4. Security Components for Implementation

An indicative list of the security components and tools considered for security solution is given below. MSI shall be responsible for deployment, integration, and commissioning as well as daily operations of all security tools and technologies in IPeG hosting environment.

S. No.	Component	Description
1.	HIPS	To protect hosts against local, application and network-based attacks. (Endpoint Installations)
2.	DLP	To identify, monitor and protect data in use, data in motion on network, and data at rest in data storage area or on endpoints.

S. No.	Component	Description
3.	Email Gateway	To prevent data loss, perform email encryption, protect against known and unknown malware. By detecting and blocking malware, spam, phishing attempts and other malicious content, can significantly reduce the number of attempted and successful attacks against an organization
4.	Web Gateway	To filter unwanted software/malware from user-initiated Web/Internet traffic. Used for black box testing or dynamic testing of the web applications
5.	API Gateway	Dedicated Server that will be the single-entry point into the system from the internet as well as internal network leveraging the APIs.
6.	Two Factor Authentication	To provide two factor authentications
7.	Patch Management Tool	To manage patches/upgrades/updates
8.	Anti-Virus	Used to prevent, detect and remove malicious software.
9.	Identity and Access Management	Centralized and standardized system that automates network management of user data, security, and distributed resources, and enables interoperation with other directories.
10.	ITAM	Asset Management tool
11.	PIM/PAM suite	To secure, manage and track user access to privileged accounts
12.	Data Masking and Redaction	To mask/redact sensitive information from documents, images, stored documents repositories.
13.	Single Sign-On	To allow users to login using a single ID and password across applications securely.
14.	Database Activity Monitoring	To independently monitor and audit all database activity, including administrator activities. To generate alerts on policy violations, provide real-time monitoring and rule-based alerting.
15.	GRC Tool	Automate governance, risk and compliance activities and provide reporting, dashboards and governance workflows for stakeholders
16.	Web Crawler	To identify relevant sensitive data in public domain (such as social registry details, number, beneficiary details, department numbers etc.)

S. No.	Component	Description
17.	External Firewall	To provide a barrier to control network traffic both into and out of organization's Internet-connected network, or between different segments of an internal network. Firewalls also provide protection against threats including denial of service (DOS) attacks.
18.	Internal Firewall	To provide a barrier to control network traffic both into and out of organization's Internet-connected network, or between different segments of an internal network. Firewalls also provide protection against threats including denial of service (DOS) attacks.
19.	Web Application Firewall	Filters, monitors and blocks HTTP traffic to and from a web application. By inspecting HTTP traffic, it can prevent attacks stemming from web application security flaws, such as SQL injection, cross-site scripting (XSS), file inclusion, and security misconfigurations.
20.	IDS/IPS	To filter unwanted software/malware from user-initiated Web/Internet traffic. Used for black box testing or dynamic testing of the web applications
21.	SSL VPN	To provide remote-access VPN capability for remote operations
22.	VA-PT Tools (Web, Network and Code Review)	• **Web Vulnerability Scanner** - Tool used for web application security. Scans and identifies vulnerabilities in web applications. • **Code Review Tool** -To conduct security code review of an application's source code in order to ensure that the application has been developed so as to be "self-defending" in its given environment. • **Network Vulnerability Scanner**- Vulnerability management tool to find security loopholes in the networks.
23.	HSM	Dedicated crypto processor that is specifically designed for protection of the crypto key lifecycle. It protects cryptographic infrastructure of organizations by securely managing, processing, and storing cryptographic keys inside a hardened, tamper-resistant device. HSM is a mandatory requirement for maintaining a Aadhaar Data Vault and digital signing of Aadhaar authentication requests.
24.	SIEM	To get full visibility of the infrastructure via logs. Provides enterprises with network security intelligence and real-time monitoring for network devices, systems, and applications. Centralized Authentication, Authorization, and Accounting (AAA or

S. No.	Component	Description
		Triple A) management for users who connect and use a network service.
25.	Network Access Control	To implement policies for controlling devices and user access to their networks. NAC can set policies for resource, role, device and location-based access and enforce security compliance.
26.	Anti-DDoS	To prevent DDoS attacks
27.	Virtual Desktop Infrastructure	To provide secure access to IPeG's Information System for internal users
28.	Anti-APT	Advanced Persistent Threat Protection solution
29.	Anti-Phishing	To prevent Phishing attacks
30.	User and Entity Behaviour	To conduct social engineering (Per User)
31.	File Integrity Monitoring	To detect potential threats with real-time alerts for changes to files, folders, registry settings, and unauthorized access

The minimum requirement specifications for the above components are given in Annexure.

3.10. Miscellaneous

3.10.1. Privacy of data

In course of the project, the MSI may collect, use, transfer, store or otherwise process information. MSI warrants that it shall process all data in accordance with applicable law and regulation. MSI further warrants that it shall process such information only for the purposes of this engagement, and shall not use or disclose such information, otherwise pursuant to purposes of the engagement.

3.10.2. Ownership of Data

The MSI undertakes that all the data generated, including logs, etc. shall be the property of Government of Chhattisgarh and MSI shall have no ownership over such data.

3.10.3. Adherence to disclosure norms

CHiPS is entitled to audit any amount claimed by the MSI in an invoice submitted to it, and/or require the MSI to disclose any document, material, data, and/or information in relation to the engagement.

3.10.4. Right for security clearance

CHiPS may execute background checks on any or all employees of the MSI who are assigned to work on the project. Such background checks will include drug screening and checks for criminal activity, credit history checks, and checks on qualifications, suitability and experience of MSI's employees before and/or during their assignment to the project under this Engagement.

3.10.5. Compliance to the Laws and Regulation of India

The MSI undertakes that during the term of this engagement, it shall comply with all applicable laws and regulations, in the performance of its obligations and hold all valid and current licenses required to perform the services, in relation to this engagement and any matter relating to them.

3.11. Project Management

MSI shall be responsible managing the engagement and ensure that the scope of work for the MSI is met to the satisfaction of CHiPS. MSI shall be responsible for, but not limited to, the following activities:

3.11.1. Setting up of Project Management Office (PMO)

The MSI should setup a project office in Raipur/ Nava Raipur within 15 days of signing agreement and should have all required equipment's (like PC, Laptop, Printers, Scanners, Network Connectivity, vehicles, stationaries etc.) for proper functioning and reporting. No additional payment shall be made in this regards and participating bidders shall have to consider the same in their Financial Bids. The MSI has to submit evidence of establishment of such office to CHiPS.

The MSI shall set-up a project management office (PMO) for the complete project term. The PMO shall consist of the Project Manager designated by the MSI and representatives of CHiPS. PMO shall formally meet every week to discuss:

(a) Project Progress
(b) Activities undertaken and planned by the MSI
(c) Delays, if any – Reasons thereof and ways to make-up lost time
(d) Issues and concerns
(e) Performance and SLA compliance reports;
(f) Unresolved and escalated issues;
(g) Change Management - Proposed changes, if any
(h) Project risks and their proposed mitigation plan
(i) Discussion on submitted deliverable
(j) Timelines and anticipated delay in deliverable, if any
(k) Any other issues that either party wishes to add to the agenda.

The operational aspects of the PMO need to be handled by the MSI including maintaining weekly statuses, minutes of the meetings, weekly/ monthly/ project plans, etc. MSI shall recommend PMO structure for the project implementation phase and operations and maintenance phase.

3.11.2. Preparation of a Tool Based Detailed Project Plan

Upon inception of the project, the MSI shall prepare a tool based detailed project plan for the engagement. The project plan shall include detailed project activities for all phases of the project, timelines for those activities, key project milestones, key resources who shall undertake the activity etc.

3.11.3. Project Status Monitoring and Reporting

The MSI shall circulate written progress reports each week to CHiPS and other stakeholders. Project status report shall include Progress against the Project Plan, status of all risks and issues, exceptions and issues along with recommended resolution etc. This project status report shall be

discussed each week by during the weekly project status meeting. Other than the planned meetings, in exceptional cases, project status meeting may be called with prior notice to the MSI. CHiPS reserves the right to ask the MSI for the project review reports other than the weekly status review reports.

3.11.4. Risk and Issue Management

The MSI shall develop a Risk Management Plan and a risk register for the engagement. MSI shall identify project risks, analyse and prioritize the risks, identify mitigation plans and document the risks and their mitigation strategy in the risk register.

The MSI must also prepare an issue management procedure to identify, track, and resolve all issues confronting the project. MSI must prepare an issue register to document all key project issues, their impact on the engagement and their resolution plans.

The MSI should periodically update risk and issue register and submit them as part of the weekly project review reports. The project risks and issues are also to be discussed with CHiPS in weekly PMO meetings in order to discuss and identify mitigation plans.

3.11.5. Change Control Management

(i) This Section describes the procedure to be followed in the event of any proposed change to a Contract Agreement ("Contract Agreement"), Project Implementation Phase, SLA and scope of work and functional requirement specifications. Such change shall include, but shall not be limited to, changes in the scope of services provided by the MSI and changes to the terms of payment as stated in the Terms of Payment Schedule.

(ii) CHiPS or its nominated agencies and the MSI recognise that frequent change is an inevitable part of delivering services and that a significant element of this change can be accomplished by re-organizing processes and responsibilities without a material effect on the cost. The MSI will endeavour, wherever reasonably practicable, to effect change without an increase in the terms of payment as stated in the payment terms and CHiPS or its nominated agencies will work with the MSI to ensure that all changes are discussed and managed in a constructive manner.

(iii) This Change Control Schedule sets out the provisions which will apply to all the changes to the Agreement and other documents except for the changes in SLAs for which a separate process has been laid out, such as:

(iv) "A notice of the proposed revision ("SLA Change Request") shall be served to CHiPS or the MSI as the case may be.

(v) This Change Control Process sets out the provisions which will apply to changes to the:

- Contract Agreement; and/or
- Project Implementation; and/or
- Operations and Management SLA"

(vi) Due to the evolving nature of the requirements and the complexity of the project, changes may be required before, during and after rollout of the IPeG system. These changes may require modification to the software, infrastructure and underlying processes and may thus have a financial impact.

(vii) MSI is required to work with CHiPS to ensure that all changes are discussed, managed, and implemented in a constructive manner.

(viii) One of the key requirements is that the MSI will be responsible for providing system availability according to defined service levels. This responsibility includes responsibility to implement upgrades, enhancements, extensions and other changes to the software application in order to maintain and extend reliable information systems, services and service delivery mechanism. It is important that changes to the computing environment and underlying infrastructure are executed in a standardized and controlled manner in order to mitigate the risk of interruptions to the services and to maintain a repository of knowledge about the current as well changed configurations as well as status of the computing environment at all times.

(ix) This section describes the procedure to be followed in the event of any proposed change to the scope of work and SLAs. Such change shall, inter alia, include:

- Requests for requirements changes (additions, deletions, modifications, deferrals) in Scope of Work (including software)
- Requests for resolving the problems in current production systems
- Requests for enhancements in current production systems
- Requests for new development projects

(x) The Change Control procedure applies to base-lined work products created or managed by the members of the project. The Change Control process excludes any work products that are still under development.

(xi) All planned or emergency changes to any component of the system shall be through the Change Management Process approved by CHiPS. The MSI needs to follow all such processes (based on industry ITSM framework). For any change, MSI shall ensure:

- Detailed impact analysis
- Change plan with Roll back plans
- Appropriate communication on change required has taken place
- Proper approvals have been received
- Schedules have been adjusted to minimize impact on the production environment
- All associated documentations are updated post stabilization of the change
- Version control maintained for software changes

(xii) The MSI shall define the Software Change Management and Version control process. For any changes to the solution, MSI has to prepare detailed documentation including proposed changes, impact to the system in terms of functional outcomes/additional features added to

the system etc. MSI shall ensure that software and hardware version control is done for entire duration of MSI's contract.

3.11.5.1. Change Control Note ("CCN")

The change requests in respect of the Contract Agreement (Contract Agreement), the Project Implementation, the operation, the SLA or Scope of work and Functional Requirement specifications will emanate from the Parties' respective Project Manager who will be responsible for obtaining approval for the change and who will act as its sponsor throughout the Change Control Process and will complete Form, provided in RFP. CCNs will be presented to the other Party's Project Manager who will acknowledge receipt by signature of the CCN.

The MSI and CHiPS or its nominated agencies, during the Project Implementation Phase during the Operations and Management Phase and while preparing the CCN, shall consider the change in the context of the following parameter, namely whether the change is beyond the scope of Services including ancillary and concomitant services required and as detailed in the Scope of Work related sections of the RFP and is suggested and applicable only after the testing, commissioning and certification of the Pilot Phase and the Project Implementation Phase as set out in this document & contract agreement.

3.11.5.2. Quotations

The MSI shall assess the CCN and complete Change Control Note (CCN) format, provided as Form of RFP. In completing the Part B of the CCN the MSI shall provide as a minimum:

- a description of the change
- a list of deliverables required for implementing the change;
- a time table for implementation;
- an estimate of any proposed change
- any relevant acceptance criteria
- an assessment of the value of the proposed change;
- Material evidence to prove that the proposed change is not already covered within the Agreement and the scope of work.

Prior to submission of the completed CCN to CHiPS or its nominated agencies, the MSI will undertake its own internal review of the proposal and obtain all necessary internal approvals. As a part of this internal review process, the MSI shall consider the materiality of the proposed change in the context of the Contract Agreement and the Project Implementation affected by the change and the total effect that may arise from implementation of the change.

3.11.5.3. Costs

Each Party shall be responsible for its own costs incurred in the quotation, preparation of CCNs and in the completion of its obligations described in this process provided the MSI meets the obligations as set in the CCN. In the event the MSI is unable to meet the obligations, as defined

in the CCN, then the cost of getting it done by third party will be borne by the MSI. The payment to the MSI for the Change Management will be done as per the process agreed by CHiPS.

3.11.6. SLA Monitoring and Reporting

The MSI shall be responsible for delivering the services described in the scope of work, as per the SLAs given in this RFP. MSI is also responsible for periodic monitoring and reporting of the SLAs. MSI should submit an SLA compliance report each month. MSI shall also be responsible for providing early warning of any organizational, functional or technical changes that might affect MSI's ability to deliver the services described in the SLA. Immediate actions should be taken to mitigate the risks or Issues, if any.

To the extent possible, SLA reporting should be undertaken using automated tools and SLA reporting should be do using the automated logs with minimal manual intervention. MSI shall define and implement a process for those SLAs that require manual intervention for measurement and reporting.

MSI shall prepare the reporting templates for SLA compliance reports and obtain sign-off from CHiPS. These reports should include "actual versus target" SLA performance, a variance analysis and discussion of appropriate issues or significant events, if any.

3.11.7. MIS Reporting and Dashboard

The MSI shall be responsible for delivering the reports as per the requirements of CHiPS. The MSI shall prepare the reporting templates and obtain sign-off from CHiPS. The MSI shall also be responsible for providing dashboards to the senior officials of CHiPS.

To the extent possible, reporting should be undertaken using automated tools minimal manual intervention. For the inputs requiring manual intervention, the MSI shall define and implement a process for measurement and reporting.

3.11.8. Compliance to SLAs

MSI shall ensure compliance to SLAs as indicated in this RFP and any upgrades/ major changes to the software shall be accordingly planned by MSI ensuring the SLA requirements are met at no additional cost to CHiPS.

The SLA Monitoring function of the solution is an important requirement of this Project. Equally important from the point of the MSI is that the applicable penalties on account of the performance are linked to a measurement of the of SLA parameters.

3.11.9. Problem Identification and Resolution

The MSI shall be responsible for problem identification and resolution. The brief details are as follows:

(i) Errors and bugs that persist for a long time, impact a wider range of users and are difficult to resolve become a problem. MSI shall identify and resolve all the application problems in

the identified solution (e.g. system malfunctions, performance problems and data corruption etc.)

(ii) Monthly report on problems identified and resolved would be submitted to CHiPS along with the recommended resolution.

3.11.10. Maintenance Configuration Information

MSI shall maintain version control and configuration information for application software and any system documentation.

3.11.11. Template Creation and Enhancements

Templates are pre-formatted documents, intended to speed up the creation of commonly used document types. Templates encourage repeatability and efficiency. It ensures that there is no waste of time and money by reworking documents/spreadsheets. Templates can be utilized and customized for various purposes and audiences.

MSI is expected to create various templates to ensure standardization and efficiency in documentation of various tasks and ensure the depth of exercise, as required. In addition to the deliverables for the project, there will be additional templates which will have to be created by MSI. While a detailed list of documents may be agreed with CHiPS at the time of implementation, a list of documents.

3.11.12. Maintain System Documentation

a. MSI shall maintain at least the following minimum documents with respect to the IPeG system:

- High level design of whole system
- Low Level design for whole system / Module design level
- System Requirements Specifications (SRS)
- Any other explanatory notes about system
- Traceability matrix
- Compilation environment

b. MSI shall also ensure update of documents of software system ensuring that:

- Source code is documented
- Functional specifications are documented
- Application documentation is updated to reflect on-going maintenance and enhancements including FRS and SRS, in accordance with the defined standards
- User manuals and training manuals are updated to reflect on-going changes/enhancements
- Standard practices are adopted and followed in respect of version control and management

c. All the project documents need to follow version control mechanism. MSI will be required to keep all project documentation updated and should ensure in case of any change, the project documents are updated and submitted to CHiPS by the end of next quarter.

d. For application support, MSI shall keep dedicated software support team to be based at MSI location that will act as a single point of contact for resolution of all application related issues. This team will receive all the application related tickets/incidents and will resolve them. This team should also comprise domain experts to provide all domain related support to technical team. In its technical proposal, MSI needs to provide the proposed team structure of application support including number of team members proposed to be deployed along with roles and skills of each such member. Application support team shall be employees of MSI.

e. Any software changes required due to problems/bugs in the developed software/application will not be considered under change control. The MSI will have to modify the software/application free of cost. This may lead to enhancements/customizations and the same needs to be implemented by the MSI at no extra cost.

f. Any additional changes required would follow the Change Control Note. CHiPS may engage an independent agency to validate the estimates submitted by the MSI. The inputs of such an agency would be taken as the final estimate for efforts required. MSI is to propose the cost of such changes in terms of man-month rate basis and in terms of Work Breakdown Structure (WBS) basis in the proposal.

g. As part of change management process, the MSI should keep all the relevant documents up-to-date.

3.12. Guidelines, Information and Other Requirements

3.12.1. Maintenance and Transfer of Documentation

The MSI shall be responsible for maintaining proper documentation related to all the above-mentioned activities, ensuring that the knowledge about planning, establishing and maintaining of entire system under the responsibility of MSI is documented and made available for reference/ knowledge transfer as and when required. The documentation is to include but not be limited to all the active and passive equipment provided, used or maintained by MSI, all applications/ software, design and operational characteristics of these systems and sub-systems, and their operations & maintenance throughout the duration of the project. Detailed diagrams/ images/ screenshots etc. are to be used as required, to illustrate suitable attributes. These activities are aimed at properly documenting the up-to-date knowhow and when required, transferring the knowledge of all of the following:-

(i) All assets including active and passive equipment along with their programming, testing and deployment

(ii) Software

(iii) Hardware

(iv) Technologies

(v) Integration

(vi) Processes

(vii) Operations

(viii) Maintenance

(ix) Any other aspects related to the project but not covered by (i) to (viii) above.

The documentation elaborated above is to be produced to CHiPS on a quarterly basis for review, reference and record. The MSI is to undertake the operations and maintenance of the system by virtue of satisfactorily carrying out the requisite set of activities, as required.

Note: All the documentation submitted by the bidder should contain an executive summary which reflect the entire report in a summarized form. The report should also contain a section which clearly defines the decisions required, risks and mitigation, etc.

3.12.2. Auditing of the Work Undertaken by the MSI

CHiPS reserves the right to carry out thorough audit of the work undertaken by the MSI at any/ all stages of the project, either on its own, or through a third party appointed by CHiPS. The payment related to Change Management will also be dependent upon the validation of updated documentation.

3.12.3. Compliance Requirements for Equipment/Systems to be Procured & Executed

(a) The items/equipment required or their specifications mentioned, if any, are indicative requirements and should be treated for benchmarking purpose only. Bidders are required to undertake their own requirement analysis and may propose higher specifications that are better suited to the requirements.

(b) Any manufacturer or product name, if mentioned in the RFP should not be treated as a recommendation for the manufacturer/ product.

(c) None of the equipment proposed by the Bidder should be End-of-Life or End-of-Support product. It is essential that the technical proposal is accompanied by the OEM certificate in the format given in this RFP, wherein the OEM will certify that the product is not end-of-life product and shall support for a minimum duration of the project term from the date of 'Commencement of Operations as per accepted solution'.

(d) Technical Proposal should be accompanied by OEM's product brochure/datasheet. Bidders should ensure complete warranty and support for all equipment from OEMs. All the back-to-back service agreements should be submitted along with the Technical Bid.

(e) All equipment, parts should be Original and New.

(f) The Successful Bidder should also propose the suitable specifications of any additional hardware, if required for the system to perform optimally.

(g) MSI is required to ensure that there is no choking point/ bottleneck anywhere in the system (end-to-end) to affect the performance/ SLAs.

(h) All necessary hardware, software, licenses etc. and IPR will be in the name of CHiPS.

3.12.4. Infrastructure Compliance Review

As required, CHiPS or its appointed representative shall have the right to perform the Infrastructure Compliance Review to verify the conformity of the Infrastructure (both IT, non-IT as well as Network infrastructure) supplied by the Master System Integrator against the requirements and specifications accepted CHiPS. The compliance review shall not absolve the MSI from ensuring that proposed infrastructure meets the SLA requirements.

3.12.5. Manageability Review

CHiPS or its appointed agency shall have the right to verify the manageability of the solution and its supporting infrastructure using suitably equipped and capable tools/ system used by the MSI for managing their services. The manageability requirements include requirements such as on line ticket monitoring, remote monitoring, administration, configuration, inventory management, fault identification etc.

3.13. Exit Management

Upon termination or end of contract, the MSI will retain its Assets excluding the software (and source code), data, plans, drawings, specifications, designs, reports, documentations, manuals, catalogues, brochures, etc. The MSI may note that the ownership of data (including logs) shall be with CHiPS and Government of Chhattisgarh. However, the MSI will have to undertake knowledge transfer to officials of CHiPS or its representatives.

3.13.1. Purpose

This section sets out the provisions, which will apply on expiry or termination of the contract. The objective is to ensure smooth transition and exit of MSI. The MSI and CHiPS shall ensure that their respective associated entities carry out their respective obligations set out in this section.

3.13.2. Exit Duration

The duration of exit management period will be three months from the date of termination or three months before the expiry of contract. CHiPS reserves the right to request MSI for project related information support for a period of one year after the end of exit management period.

3.13.3. Exit Management Plan

MSI shall provide CHiPS with a recommended exit management plan ("Exit Management Plan") which shall deal with at least the following aspects of exit management in relation to the SLA as a whole and in relation to the Project Implementation, the Operation and Management SLA and Scope of work definition

- A detailed program of the transfer process that could be used in conjunction with a new MSI including details of the means to be used to ensure continuing provision of the services throughout the transfer process or until the cessation of the services and of the management structure to be used during the transfer;
- Plans for the communication with such of the MSI, staff, suppliers, customers and any related third party as necessary to avoid any material detrimental impact on IPeG project's operations as a result of undertaking the transfer;
- Plans for provision of contingent support relating to project related information support to CHiPS and new MSI for a period of one year after the end of exit management period.
- MSI shall re-draft the Exit Management Plan annually thereafter to ensure that it is kept relevant and up to date.
- The Exit Management Plan presented by the MSI shall be approved by CHiPS
- In the event of termination or expiry of SLA, Project Implementation, Operation and Management SLA or Scope of Work each Party shall comply with the Exit Management Plan.
- During the exit management period, the MSI shall use its best efforts to deliver the services.
- Payments during the Exit Management period shall be made in accordance with the Terms of Payment Schedule.
- The terms of payment as stated in the RFP include the costs of the MSI complying with its obligations under this Schedule.

This Exit Management plan shall be furnished in writing to CHiPS within 30 days from the receipt of notice of termination or four months prior to the expiry this Agreement.

3.13.4. Transfer of Deliverables and Documents

1. MSI shall submit all the deliverables as per the contract. All such deliverables will be submitted to CHiPS to ensure the documentation of entire project history is available for ready reference.
   - Source code & object code for custom applications/ IPeG platform, customization on COTS products, Intellectual Property Rights and related documentation, all other relevant materials, artefacts etc.
   - Deliverables updated including due to reasons of Change Management
   - User manuals
   - Test documents (test cases, test data, test scripts, etc.) including approved UAT plans, approved UAT criteria documents, UAT certificates
   - Training documents including training plans, training feedback forms, textual and audio-visual training content, and training completion certificates
   - Report on data handover (masters, transactions, logs, etc.) to CHiPS

2. In addition to the above, the MSI has to make available the below documents to ensure completeness of documentation:
   - Functional Requirements Specifications
   - Approved High-Level and Low-Level Design Documents
   - Software Specifications Document including data models
   - SLA Compliance Reports and performance monitoring reports
3. MSI shall also deliver to CHiPS all documents provided by or originating from the IPeG project and all documents produced by or from or for MSI in the course of performing the activities as per the contract.
4. After receiving all the deliverables and documents mentioned in this section, CHiPS will give the signoff to MSI against exit management. Inability to furnish any of these documents will lead to penalty with the maximum value of 1% of contract value.

3.13.5. Transfer of Agreements and Licenses

On request by CHiPS, MSI shall carry out such assignments, transfers, licenses and sub-licenses as MSI may require in relation to maintenance or service provision agreement between MSI and third party lessors, vendors, and which are related to the services and reasonably necessary for the carrying out transition by MSI and new MSI.

For cloud/ infrastructure hosting services in case CHiPS has continued with CSP of MSI as per section 3.8.1 “Hosting Strategy for IPeG” any of the below scenarios may be applicable during exit:

1. CHiPS may decide to continue with the cloud service provider as utilized by the MSI – In this case MSI shall ensure the agreement transfer of the CSP with CHiPS or its nominated agency (new MSI) on prevailing terms and conditions as per year 3.
2. CHiPS may decide to procure hosting services from an alternated cloud service provider/ SDC cloud – In this case MSI will be responsible to assist new MSI in migrating the solution to new environment as part of Hand Over - Take Over signoff.

3.13.6. Knowledge Transfer

The brief description about the Knowledge Transfer is provided below:

A. <u>Overview</u>

- **Team Composition**: The Knowledge Transfer (KT) team will comprise of resources from MSI.
  - CHiPS will identify and deploy the resources for supervising the KT activity. The resources will also be trained on operations and maintenance activities with an aim to operate and maintain IPeG after the exit of MSI.
  - MSI will identify and deploy the functional and technical Subject Matter Experts (SMEs). The team should comprise of resources who understand IPeG and have

contributed to the development and maintenance. The team comprising of such resources along with SMEs will do the KT as per the agreed KT plan

- New MSI will identify and deploy the resources for participating in the KT activity. The resources should be functional as well as technical. New MSI should ensure that the resource it plans to deploy for customization, integration, installation, commissioning, troubleshooting, operations and maintenance of IPeG take part in KT exercise.

- **Deployment Schedule:** A detailed deployment schedule will be prepared by MSI for the identified resources. This deployment schedule will have well-defined milestones as per the progress of the KT exercise. As per the deployment schedule, all the concerned parties will deploy its identified resources.

- **Documentation**: MSI will share all detailed documentation with CHiPS at least one week before the commencement of KT exercise.

- **Logistics**: The expenses related to boarding and lodging of MSI to be borne by it during the KT period.

- **Venue**: In the KT plan, MSI will specify the pre-requisites of venue for KT exercise. The MSI will finalize the necessary arrangements required for KT venue in consultation with CHiPS. After acceptance of KT plan by CHiPS, MSI will be responsible to make necessary arrangements (such as projector, laptop/desktop, internet connection, printed copies of documentation, writing pads, pens, etc.)

- **Language**: The language of documentation as well as KT exercise will be English.

B. Components of Knowledge Transfer

- **Understanding of IPeG:** To begin with, the KT will cover the overall understanding of scope of IPeG. Under this category, a high-level understanding of various components of IPeG and their interdependencies will be covered

- **Understanding of IPeG Functionalities & Features:** After an initial understanding, the KT will cover the detailed understanding of functionalities and features of different components of IPeG. Under this category, a comprehensive functional understanding will be provided

- **Understanding of Technology Stack and Tool Stack:** After the functional scope, the KT will cover the overall understanding of technology components i.e. technology stack, tools and techniques adopted in IPeG. Under this category, a detailed understanding will be provided on licensing, configuration, best practices, common mistakes, FAQs, scalability and performance tuning of IPeG

- **Source Code learning: MSI** will be responsible for providing a detailed understanding of the source code of IPeG and customization done on COTS products. MSI will also support by answering the questions of new MSI, if any.

- **Deployment and Setup training:** After understanding on source code including test automation scripts, new MSI will be assisted by MSI on deployment, setup and configuration of IPeG.

- **End to End Test Scenario Preparation to be done by MSI:** The end to end functional test scenarios for IPeG will be prepared by the MSI.

- **Troubleshoot issues during MSI testing:** For troubleshooting during the testing, MSI will provide process documents and templates for IPeG. The documents and templates should also assist MSI in determining whether the bug must be fixed by MSI.

- **Reverse KT by new MSI:** Before finalization of KT, new **MSI** will carry out the reverse KT to the MSI. This exercise will be done with the intent to ensure that new MSI has developed accurate and sufficient understanding of IPeG to customize, integrate, install, commission, troubleshoot, operate and maintain the IPeG with minimal support from MSI.

- **KT acceptance criteria definition for each session:** For each session, a detailed acceptance criterion will be jointly prepared by new MSI and MSI. However, CHiPS will have rights to add, modify, or remove any criteria it deems fit. The acceptance criteria will be finalized before the commencement of knowledge transfer. In case any acceptance criteria are deemed irrelevant, CHiPS will have the rights to waive the concerned criteria.

- **Exit and Closure of KT:** At the end of KT exercise, a report will be submitted by MSI which will list down the observed quality against the defined acceptance criteria. In case all the acceptance criteria are met, CHiPS will grant the sign-off of KT to the MSI. In case some of the acceptance criteria are not met, CHiPS will review the relevance of such criteria. For the criteria which are not met but considered relevant, the MSI will repeat KT exercise and resubmit a revised report. The process will get repeated till all the relevant acceptance criteria are met by MSI. At any time, CHiPS will have the right to seek the feedback of KT exercise from the new MSI.

C. Mode of Knowledge Transfer

For KT exercise, a variety of modes will be adopted. Some of the modes of KT to be adopted by MSI are described below:

- **Manuals and Documents:** For each session of KT, the relevant documentation will be shared by MSI with the new MSI and CHiPS. The documentation will comprise of manuals and other documents. The manuals will be related to user manual, training manual, setup guide, troubleshooting manual.
- **Presentations:** For each session of KT, self-explanatory presentation will be shared by MSI with the new MSI and CHiPS. For topics requiring further study, the references and links to relevant documentation will be provided as part of the presentation.

D. Additional Information about Software Source Code Handover

The MSI should ensure the following:

- There should be proper documentation and commenting on source code
- The source code should have file and folder organization, consistent naming and structure, etc.
- The source code should be easy to read, should not be obfuscated and should follow industry best practices
- The third-party libraries should be provided along with source code
- The following should be supplied
    - list of known defects
    - list of incident and problem records
    - details on the last two releases (implementation time, increased incidents following the release, etc.)
    - stability of source code base
    - integration points and the contacts for necessary support
    - expected growth of the file system / database / message queues
    - third party dependencies and contact details
    - scalability and performance matrices
- Technology stack
- Disaster recovery component
- System backups and restoration strategy and responsibility
- Batch processes and their schedules
- Major incident management process for the application
- Stakeholders notification processes of changes and outages
- Agreed outage periods / times
- Tool and infrastructure for source code repository, and backup/restoration and change management
- Deployment target (Development, Staging, etc.)
- The third-party licenses, their prices, and date & frequency of renewal
- Common troubleshooting problems or complaints and their resolution
- Details about last security audits undertaken
- Documentation for the target infrastructure and network
- Severity and impact from recent incidents
- Developer workstation setup instructions

- Development aides and frameworks used and details of their licenses

The MSI shall be required to demonstrate the following:

- build the code successfully
- build unit tests and make all pass
- execute other tests successfully, and all pass (acceptance, integration, etc.)
- database of open issues
- product runs (installation instructions)

3.13.7. Confidential Information, Security and Data

MSI will act promptly on the commencement of the exit management period supply to CHiPS the following:

- Source code, object code, Intellectual Property Rights and related documentation, all other relevant materials, artefacts etc. to CHiPS. CHiPS shall own all IPR of the material provided;
- All current and updated data for purposes of CHiPS transitioning the services to the new MSI;
- All other information (including but not limited to documents, records and agreements)
- Related to the services reasonably necessary to enable CHiPS, or new MSI to carry out due diligence in order to transition the provision of the services to CHiPS or its nominated agencies, or new MSI (as the case may be).
- Before the expiry of the exit management period, MSI shall deliver to CHiPS all new or updated materials as required by CHiPS and mentioned in this section and shall not retain any copies thereof. Any publicity/use of material for any other engagement will require prior approval from CHiPS.

3.13.8. Data migration support

- During the exit management period, MSI will provide information required by the new MSI, for successful completion of transition. MSI shall furnish the information requested within three working days. Information request will be considered to be accepted and completed after CHiPS's approval.
- Penalty on Exit management period payment on non-cooperation with new MSI will be 5% of total amount to be paid against bills submitted during exit management period for each such instance of non-provision of information request by CHiPS/new MSI within three working days from the date of request.

3.13.9. Rights of Access to Premises

- At any time during the exit management period, where assets are located at MSI's premises (if any), MSI will be obliged to give reasonable rights of access to (or, in the case assets are located on a third party's premises, procure reasonable rights of access to) CHiPS and/or new MSI in order to make an inventory of the assets
- MSI shall also give CHiPS or new MSI right of reasonable access to MSI's premises and shall procure MSI or new MSI rights of access to relevant third party premises during the exit management period and for such period of time following termination or expiry of the agreement as is reasonably necessary to migrate the services to CHiPS, or new MSI

3.13.10. General Obligations

- MSI shall provide all such information as may reasonably be necessary to affect as seamless a handover as practicable in the circumstances to CHiPS or new MSI and which MSI has in its possession or control at any time during the exit management period.
- For the purposes of Exit Management, anything in the possession or control of MSI or associated entity is deemed to be in the possession or control of MSI.
- MSI shall commit adequate resources to comply with its obligations under Exit Management.

3.13.11. Payments

- For the last one quarter (three months), the payment to the MSI will be done as per the payment terms with deductions as applicable for non-compliances during exit management period and SLA will be levied by CHiPS on MSI.
- Payment to MSI shall be made to the tune of the bills submitted for payment, after successful verification of the supporting documents required to be submitted along with each bill.

3.13.12. Completion of Service for Billing

- For L1 support, the MSI needs to submit monthly reports derived from centralized helpdesk for assessing delivery of service
- For L2 support, following documents will be required for assessing completion of service:
  - Monthly summary of calls forwarded and resolved / call-wise turn-around-time / Service Reports derived from centralized helpdesk system against each L2 resource
- For L3 support, following documents will be required for assessing completion of service:
  - Submission of monthly summary of total calls logged and resolved during the month along with service report from requested who has requested for resolution of issue (monthly basis)

3.13.13. Submission of Signed handover-takeover Document

- MSI will be required to submit handover and takeover document in coordination with CHiPS and new MSI, duly signed by authorized representative of CHiPS and new MSI.
- Non-submission of hand-over take-over document, will correspond to non-completion of exit management.

3.13.14. Support to be extended by MSI

MSI shall provide access to CHiPS to all information held or controlled by them which they have prepared or maintained in accordance with the agreement for the contract under this project and subsequent amendments thereof. Such information shall include details pertaining to the services rendered and other performance data.

1. During the exit management period, MSI will provide information required by CHiPS or new Master System Integrator, hereinafter referred to as “new MSI” for successful completion of transition. MSI shall furnish the information requested **within three working days**. Information request will be considered to be accepted and completed after CHiPS’s approval.
2. Non-cooperation with new MSI for provision of information request by CHiPS/new MSI, within above mentioned duration from the date of request (if applicable), will be treated as non-compliance and pending payments will be withheld till corrective actions are taken by MSI
3. MSI will submit one copy each of project history to CHiPS. The project history includes the following documents:
    - All deliverables
    - All documents related to the project(s)
    - All invoices and supporting documents
    - Details of all resources deployed during the contract period (including qualification, experience at the time of being deployed on the project, start date, end date)
    - CVs of all resources deployed during the Exit Management period
    - Attendance related details of L1, L2 and L3 resources during the contract period.
    - Approvals if any taken from CHiPS or information furnished, if any, to CHiPS about replacement of resources.

3.13.15. Transition Closure

Once all requirements are fulfilled and transition is approved by CHiPS, the formal closure for transition can be carried out and exit management may be considered to be completed. At the end of exit management period, payments will be made as per the payment terms defined in the RFP.

3.14. Business and Technical Services (Scheme onboarding services)

The business and technical services mentioned in the Section 3.1. For this purpose, a dedicated team of the MSI is expected to be deployed in CHiPS on full-time basis from the date of Go-Live.

3.14.1. Handholding support for adoption of platform component(s) in their existing department applications

Once the solution component has been developed by the MSI, the departments will have a choice to adopt one or more solution components they wish to utilize. The roles and responsibilities of the MSI for handholding support to the departments for adoption of platform components is described along with the concerned components.

- Prepare and maintain the training material
- Conduct functional trainings to master trainers from CHiPS (in-house staff) to enable them to coordinate with departments on functional aspects
- Prepare and maintain the user manual for end-users including administrators
- Prepare and maintain the integration documents to be consumed by developers and other technical staff of the department(s)

In addition, the roles and responsibilities for handholding support to specific departments are summarized below:

- Technical assessment for migration of existing content of the component
- Technical assessment, guidance and support for integration of the component

Note: The MSI will not be responsible to make any software modifications in the existing systems of the departments interested in using the IPeG components. However, in some cases, the Business and Technical Services team of MSI may be utilized for some activities like API creation, etc.

3.14.2. Support for Data Quality Assessment and Data Cleansing

The MSI should support the departments in getting their data quality assessment. To do this, the MSI will have to perform the below activities:

- The MSI should help the department upload the data in the IPeG or integrate the database and the relevant table / datasets with the IPeG.
- The MSI will have to assist the departments in configuration of visualization, if any.
- The MSI should help in providing clarification to the departments w.r.t. to the reports generated for analysing data quality
- The MSI will have to suggest data cleaning processes and activities that needs to be undertaken
- With approval from CHiPS and concerned department, the MSI will have to undertake assessment of data quality and carry out the data cleansing exercise, if any.

3.14.3. Registry Creation and Data Integration (for data owners)

For schemes, there may be a requirement to create registries (e.g. list of colleges, students, etc.) which can be used for various purposes including reference and verification. The MSI will be responsible to create registries. There may be two scenarios:

- **Digitized Database**: These registries may be already available in form of a database. In such case the MSI will need to Support for Data Quality Assessment and Data Cleansing (Section 3.14.2) and integrate the same with through creation of APIs (Create, Read, Update and Delete).
- **Electronic files/paper-based lists**: These registries may have to be digitized before being available for usage. In such case, the MSI will need to create registry, create APIs (Create, Read, Update and Delete), upload electronic files (excel, etc.) and train the user department in data entry/correction process.

For each of the data field in social registry, a master-of-data may be defined. There may be two scenarios:

- **Digitized Field**: The data field may be already available in form of a database. In such case the MSI will need to Support for Data Quality Assessment and Data Cleansing (Section 3.14.2), assist in Aadhaar Vaulting, and integrate the same with through creation of APIs (Create, Read, Update and Delete).
- **Electronic files/paper-based lists**: These registries may have to be digitized before being available for usage. In such case, the MSI will need to create registry, create APIs (Create, Read, Update and Delete), upload electronic files (excel, etc.), assist in Aadhaar Vaulting and train the user department in data entry/correction process.

4. MANPOWER DEPLOYMENT

4.1. Guidelines for staffing and provisioning of manpower

(i) Implementation of IPeG System is envisaged offsite at MSI's premise wherein, a dedicated core team shall be stationed at the CHiPS's premises while the development is conducted.

(ii) The bidder shall provide a detailed staffing schedule in their Technical Proposal as per the format provided as part of this RFP.

(iii) The staffing schedule should also include an Organization Chart showing the proposed organization to be established by the MSI for execution of the scope of work. The organization chart should clearly bring out variations to the Organization structure if any envisaged by the MSI for various phases/stages of the project.

(iv) Separate organization structure should be provided for clearly identifiable activities such as Development of IPeG System, call centre management etc.

(v) Detailed CVs should be provided for key profiles that will be subject to evaluation. CVs should be as per the CV format given in this RFP. Area of expertise, role and tasks assigned should be clearly identified for each of the key profiles. CHiPS might interact with the said resources and this interaction shall be considered in technical evaluation.

(vi) Key roles in the MSI's team should be held only by Permanent employees of the MSI

(vii) The Staffing Schedule should contain the schedule of deployment of the Key personnel. It should also clearly highlight onsite and offsite effort of each profile.

(viii) The CHiPS shall approve this schedule after its careful study and may ask the MSI to make the changes in the schedule, if required.

(ix) The infrastructure or other facilities required for the efficient execution of work under the Contract, should be provided by MSI to its employees who are working under this contract.

4.2. Replacement of Personnel

(i) The MSI should to the best of its efforts, avoid any change in the organization structure and proposed manpower proposed for execution of the scope of services or replacement of any manpower resource.

(ii) If the same is however unavoidable, due to circumstances such as the resource leaving the MSI's organization, MSI shall promptly inform the CHiPS in writing, and the same shall require subsequent approval by the CHiPS. MSI should ensure that they adhere to the SLA for replacement of manpower as defined in this RFP.

(iii) In case of Key Management Personnel, the proposed manpower should score same or more marks as obtained at the time of technical evaluation by the concerned resource. In

case of resources other than Key Management Personnel, the proposed manpower should have equivalent education qualification, relevant experience, and certification(s) as per RFP.

(iv) In case of replacement of any manpower resource, the MSI should ensure efficient knowledge transfer from the outgoing resource to the incoming resource and adequate hand-holding period and training for the incoming resource in order to maintain the continued level of service.

4.3. Removal of Personnel

(i) CHiPS may at any time object to and request the MSI to remove from the sites any of MSI's authorized representative including any employee of the MSI or his team or any person(s) deployed by MSI or his team for professional incompetence or negligence or for being deployed for work for which he is not suited.

(ii) CHiPS's representative shall state to the MSI in writing his reasons for any request or requirement pursuant to this clause. The MSI shall promptly replace any person removed, pursuant to this section, with a competent substitute, and at no extra cost to the CHiPS.

4.4. Logistics requirements of the Personnel

The MSI shall be responsible for the deployment, transportation, accommodation and other requirements of all its employees required for the execution of the work and provision of services for all costs/charges in connection thereof.

4.5. Escalation Matrix

(i) As part of the technical proposal, the bidder shall provide a detailed Escalation Matrix mapping back to the MSI's organizational structure proposed.

(ii) The Escalation Matrix should address key requirements stated in the Service Level Agreements for various service delivery activities and cover all major service delivery activities.

(iii) The triggers for escalation should be clearly identified and stated for each category of service in the Technical Proposal.

(iv) The MSI will also prepare the Escalation Matrix for support relating to CHiPS

4.6. Manpower Qualification and Experience Requirement

(i) The MSI has to deploy well qualified and experienced resources having in-depth knowledge and experience of the position for which they are deployed. The resources shall have to

carry out the scope work in order to implement the IPeG System and meet the service levels defines as part of this RFP.

(ii) A bare minimum qualification and experience requirements of the key resources to be deployed, are given in Section 4.10, along with the indicative high-level roles and responsibilities of the resources which they are expected to carry out objectively while meeting the SLA requirements.

4.7. CHiPS's Role and Responsibility

During project duration the CHiPS shall have following roles and responsibilities:

(i) CHiPS will provide basic office amenities to the MSI's personnel (except call centre staff) at its office locations for performing their part of the obligations as outlined in the terms of reference.

(ii) All the facilities provided by CHiPS are promised to be available only for the time period as agreed upon by MSI and CHiPS as the official work time and workdays.

(iii) Beyond the time frame contractually agreed upon, MSI will not be entitled to any of these facilities.

(iv) CHiPS will provide the following infrastructure and no other facilities beyond this scope mentioned.

a. Office space for onsite manpower including Seating Facility that includes desks and chairs for this number of staff.

b. Server Room & Communication Room for Connectivity

c. LAN connectivity, Network printing facility, Electrical Connectivity.

(v) Coordination between all the divisions/departments for providing necessary information for the study and development/customization of the necessary solution.

(vi) Provide necessary support to MSI for conducting workshops for the Stakeholder departments, if any.

(vii) Monitoring of overall timelines, SLAs and calculation of penalties accordingly.

(viii) Conducting UAT for the application solution deployed.

(ix) Issuing the Acceptance Certificate on successful deployment of the software application and for other components of the Scope of Work (wherever required).

(x) Any other requirements that could arise during operations for effective governance and to meet any administrative requirement.

(xi) Ensuring the staff members and other stakeholders attend the training programs as per the schedule defined by MSI and agreed upon by the CHiPS.

(xii) Provide sign off on the deliverables of the project within agreed timelines.

4.8. Key Resources of MSI

The MSI should propose the key resources and map their positions across following teams. An indicative team structure for implementation of IPeG System is given below in the subsequent sections. The MSI may re-organize the team structure or deployment of staff and their position as per the proposed IPeG System. The indicative team categories and positions are provided in the following categories:

1. Leadership Unit (Key Management Personnel)
2. Architect Unit (Key Management Personnel)
3. Track Leads (Key Management Personnel)
4. Hosting Infrastructure
5. Operations Team

The team requirement for above mentioned categories is defined in the table given below:

#	Key Resource Category	Implementation Phase	O&M Phase
Leadership Unit			
1	Project Manager	1	1
Architect Unit			
1	Solution Architect	1	-
2	Security Architect	1	-
3	Data Architect	1	-
4	Cloud / Hardware Infrastructure Architect	1	-
Track Leads			
1.	Track Lead – Application Manager	-	1
2.	Track Lead – Security and Privacy	-	1
3.	Track Lead – Data Analytics	1	1
4.	Track Lead – Aadhaar	1	-

#	Key Resource Category	Implementation Phase	O&M Phase
Technical support Team			
1	Server and Storage Administrator	-	1
2	Network and Security Administrator	-	1
3	Database Administrator	-	1
4	Call Centre Agents including 1 supervisor	-	5
5	IT Helpdesk Agents including 1 supervisor	-	3
6	Security and Privacy Expert	-	1
Software Team for Solution Development, COTS customization &Scheme onboarding.			
1.	Solution development Team to meet the timelines of the project (Developers, Testers etc.)	As per MSI's solution requirements	As per MSI's solution requirements

Table 2: Indicative Resources

A minimum qualification and experience requirements of the key resources to be deployed, are given in Section 4.10, along with the indicative high-level roles and responsibilities of the resources which they are expected to carry out for meeting the service levels.

4.9. Manpower Deployment Schedule

The MSI has to deploy well qualified and experienced resources having in-depth knowledge and experience of the position for which they are deployed. The resources shall have to carry out work in order to meet the desired objectives of implementing and running the IPeG System. The table given below provides an indicative manpower deployment schedule. In its technical bid, the bidder has to take into account the scope of work, timelines, service levels and other requirements defined in the RFP and propose a detailed manpower deployment plan. This deployment plan, for each role should provide clear description of the effort (in hours/day), location (onsite/offsite), deployment (full-time or part-time), etc.

#	Key Resource Category	Phase	Description
Leadership Unit			
1	Project Manager	Implementation	Onsite full-time
		O&M	Onsite full-time

#	Key Resource Category	Phase	Description
Architect Unit			
1	Solution Architect	Implementation	Onsite full-time
		O&M	Not applicable
2	Security Architect	Implementation	Onsite full-time during design phase
		O&M	Not applicable
3	Data Architect	Implementation	Onsite full-time
		O&M	Not applicable
4	Cloud Architect	Implementation	Onsite full-time
		O&M	Not applicable
Track Leads			
1	Track Lead – Application Manager	Implementation	Onsite full-time
		O&M	Not Applicable
2	Track Lead – Security and Privacy	Implementation	Onsite full-time after design phase
		O&M	Not Applicable
3	Track Lead – Data Analytics	Implementation	Onsite full-time
		O&M	Onsite full-time
4	Track Lead – Aadhaar	Implementation	Onsite full-time
		O&M	Not Applicable
Technical support team			
1	Server and Storage Administrator	Implementation	
		O&M	Onsite/ Offshore as proposed by bidder
2	Network and Security Administrator	Implementation	
		O&M	Onsite/ Offshore as proposed by bidder

#	Key Resource Category	Phase	Description
3	Database Administrator	Implementation	
		O&M	Onsite/ Offshore as proposed by bidder
4	Call Centre Agents	Implementation	
		O&M	Onsite at the call centre
5	IT Helpdesk Agents	Implementation	
		O&M	Onsite at the helpdesk
6	Security and Privacy Expert	Implementation	
		O&M	Onsite/ Offshore as proposed by bidder
Software Development, Operations and Maintenance Team			
6	Additional Software Development Team to meet the timelines of the project (Developers, Testers etc.)	Implementation	Onsite /Offshore full-time as proposed by bidder
		O&M	Onsite /Offshore full-time as proposed by bidder

Table 3: Indicative Manpower Deployment Schedule

4.10. Manpower Requirements

The MSI has to deploy well qualified and experienced resources having in-depth knowledge and experience of the position for which they are deployed. The resources shall have to carry out work in order to meet the desired objectives of implementing and running the IPeG System. The table given below provides the minimum qualification details of the required manpower. The MSI is expected to adhere with the requirements and deploy relevant resources for the project.

#	Key Resources	Minimum requirements
1.	Project Manager	• Minimum Education: Post-Graduation (MBA or equivalent Masters' degree) and Graduation (B. Tech., B.E.) • Total Work Experience: At least 12 years • Languages known English and Hindi • Prior project management experience of at least 10 years of handling large and complex IT/ITeS projects, with at least one large scale IT project • Should have project management experience of IT projects in government sector
2.	Architects	• Minimum Education: Post-Graduation (MTech., M.E., or equivalent Masters' degree) and Graduation (B. Tech., B.E.) • Total Work Experience: At least 10 years • Languages Known: English • Should be expert in architecture • Should be expert subject matter knowledge of their respective domains • Prior project experience in the capacity of architects in their respective domains in at least 3 large-scale IT/ITeS projects Note: For definition of large-scale IT/ITeS projects for specific roles, please refer to Section 2.11.5 of Volume-1 of this RFP.
3.	Track Leads	• Minimum Education: Post-Graduation (MCA, M. Tech, M.E.) and Graduation (B. Tech., B.E., B.C.A.) • Total Work Experience: At least 7 years • Languages Known: English and Hindi • Project experience of providing expertise related to their domain in at least 2 large-scale IT/ITeS projects Note: For definition of large-scale IT/ITeS projects for specific roles, please refer to Section 2.11.5 of Volume-1 of this RFP.
4.	Administrators	• Minimum Education: Any Graduation (Preferably B. Tech., B.E., B.C.A, B.Sc.) • Total Work Experience: At least 5 years • Languages Known: English and Hindi • Project experience of providing expertise related to their domain in at least 2 projects

#	Key Resources	Minimum requirements
5.	Call Centre Agents	• Minimum Education: Graduation (any discipline) • Call Centre Experience of at least 2 years • Should have experience in government projects in similar role • Should have worked in similar roles in large scale IT project • Effective verbal communication skills (English and Hindi)
6.	IT Helpdesk Agents	• Minimum Education: Graduation (B. Tech., B.E., B.C.A.) • Experience of diagnosing hardware and software malfunctions, troubleshooting problems, replacing hardware and software installation. • Should have experience in government projects in similar role • Should have worked in similar roles in large scale IT project • Effective verbal communication skills (English and Hindi)
7.	Security and Privacy Expert	• Minimum Education: Post Graduation (M.E./M. Tech./M.B.A./M. S or equivalent with specialization in security) and Graduation (B. Tech., B.E.) • Experience of diagnosing security incidents, troubleshooting problems, replacing hardware and software installation • Should have experience in government projects with role on security aspects • Should have worked in similar roles in large scale IT project • Effective verbal communication skills (English and Hindi)
8.	Lead Business Analyst	• Minimum Education: Post-Graduation (MBA or equivalent Masters' degree) and Graduation (B. Tech., B.E.) • Total Work Experience: At least 10 years • Languages Known: English and Hindi • Prior Business Analyst experience of at least 5 years of handling large and complex IT projects, with at least one large scale IT project • Should have similar experience in government projects • Excellent writing, communication, time management, supervision, and multi-tasking skills

#	Key Resources	Minimum requirements
9.	Analytics Expert (Data Scientist)	• Minimum Education: Post-Graduation (MCA, M. Tech, M.E.) and Graduation (B. Tech., B.E., B.C.A.) • Should have a relevant data science degree/ Certification • Total Work Experience: At least 7 years • Languages Known: English and Hindi Project experience of providing expertise related to their domain in at least 2 projects
10.	Sr. Developers	• Minimum Education: Graduation (B. Tech., B.E.) • Total Work Experience: At least 5 years of experience in software application development, programming languages and databases in the quoted technologies
11.	Developers	• Minimum Education: Graduation (B. Tech., B.E.) • Total Work Experience: At least 3 years of experience in software application development, programming languages and databases in the quoted technologies
12.	Testers	• Minimum Education: Graduation (B. Tech., B.E.) • Total Work Experience: At least 3 years of experience in software application testing in the quoted technologies

5. IMPLEMENTATION APPROACH AND PLAN

The scope of work for the MSI spans the complete Software Development Life Cycle from designing, developing, testing, maintaining and supporting the IPeG System. MSI shall work closely with CHiPS during the software implementation, maintenance and enhancement phase to ensure successful implementation and operations of the IPeG System. Implementation of IPeG System is envisaged to be rolled out in the following iterations:

Milestone No.	Component	Timeline (in Months)
I	Team Mobilization and Kick-off Meeting Design document of all components (Inception Report and Project Plan)	T +1 months
II	Establishment of hosting infrastructure required for milestone II Go-Live of Toolkits – Service Delivery Application Go-Live of Toolkits – Data Collection Tool	T + 3 months
III	Establishment of additional hosting infrastructure required for milestone III Go-Live of Identity related platform services Go-Live of Data related platform services Go-Live of Data Sources (all) including Social Registry (except Federated Part) Go-Live of Data Exchange Gateway	T + 4 months
IV	Establishment of additional hosting infrastructure required for milestone IV Go-Live of Social Registry (except Federated Part) and other data sources for 5 shortlisted schemes (refer section 3.2.3) Go-Live of Payment related platform services Go- Live of Access Channel - Common Services Portal	T + 6 months

Milestone No.	Component	Timeline (in Months)
	Onboarding of all 5 schemes to the different technology components gone live	
V	Establishment of additional hosting infrastructure required for milestone V	T + 8 months
	Go-Live of Toolkit – Scheme Analysis and Policy Planning Tool	
	Go-Live of Toolkit – Grievance Management	
	Go-Live of Toolkit – Advanced Analytics Tool	
	Go-Live of Platform Services (all remaining)	
	Go-Live of Access Channels (all remaining)	
	Go-Live of Internal Components (all)	
	Onboarding of 5 shortlisted schemes to the new technology components gone live	
VI	STQC certification of all components (including fixes)	T+12 months
	Security audit certification of all components (including fixes)	
VII	Onboarding remaining schemes to IPeG technology components	T+12 months
VIII	Operation and Maintenance of entire solution	Continued till T + 36
	Operation and Maintenance of onboarded schemes	

**Where T is the date of signing of contract with the MSI*

In order to carry out the scope of the engagement, MSI shall be required to deploy experienced and skilled manpower as per the minimum requirements mentioned in this RFP.

6. ANNEXURE

6.1. Annexure-I: Inputs For Workload Analysis

These estimates are being provided for the reference of the bidder, the actual volumes may vary based on a variety of factors including but not limited to resident behaviour, services uptake, onboarding of stakeholders, project rollout, etc. For the purpose of preparation of bid response, the bidders are encouraged to conduct their own analysis and utilize their own assumptions.

6.1.1. Access Channels Usage

The usage assumed for the purpose of budgeting is provided below:

Item	Eligibility Check	Application	Status Check	Output	Average
Self-Service (Internet)	1%	1%	1%	1%	1%
Self-Service (Mobile)	29%	20%	29%	20%	25%
Assisted (Service Delivery Outlets)	20%	78%	20%	78%	49%
Assisted (Call Center)	50%	1%	50%	1%	26%
	100%	**100%**	**100%**	**100%**	**100%**

6.1.2. Basic Details

Category	Assumption	Count
Days	Calendar	365
	Working Days	300
	Working Hours (10 am to 6 pm)	8
Districts	Divisions	4
	Districts	28
	Sub-District (Tahsil)	150

Category	Assumption	Count
	Urban Local Bodies	160
Population	Population of Chhattisgarh (2011)	2,55,00,000
	Population of Chhattisgarh (Estimated 2021)	3,12,60,450
	Households (Assumed at 4.25 members per household)	73,55,400
Beneficiaries	Beneficiaries (Average nos. on per scheme basis)	1,00,000
	Beneficiaries (Average nos. on per service basis)	26,000

6.1.3. User Estimation

Category	Assumption	Count
Assisted Service Delivery	Service delivery outlets	7,000
	Call Centre	As per RFP
	Helpdesk	As per RFP
Approvers	Department HQ (Estimated at 1 per scheme)	50
	Department Field (Estimated at 3 per scheme)	150
Portal Logins	Average Nos. of Logins (including citizens) Per Day	10,000

6.2. Annexure-II: Functional Requirements Specification

Sl #	Components	Functional Specification	Compliance (Y/N – Page reference of data sheet/ proposal)
1.	IPeG Web Portal	As per Section 3.2.4.1. Access Channels - IPeG Web Portal (Common Services Portal)	
2.	IPeG Mobile Application	As per Section 3.2.4.2. Access Channels - IPeG Mobile Application	
3.	CG State DBT Portal	As per Section 3.2.4.3. Access Channels – CG State DBT Portal	
4.	IPeG Call Centre	As per Section 3.2.4.4. Access Channels - IPeG Call Centre	
5.	IT Helpdesk	As per Section 3.2.4.5. Access Channels – IT Helpdesk	
6.	Enterprise Monitoring System	As per Section 3.2.5.1. Internal Components – Enterprise Monitoring System	
7.	Performance management & Fraud Detection	As per Section 3.2.5.2. Internal Components – Performance management & Fraud Detection	
8.	Aadhaar Authentication	As per Section 3.2.5.3. Internal Components – Aadhaar Authentication	
9.	Data Exchange Gateway	As per Section 3.2.5.4. Internal Components – Data Exchange Gateway	
10.	Single Sign-on Tool	As per Section 3.2.5.5. Internal Components – Single Sign-on Tool	
11.	Identity Authentication Service	As per Section 3.2.2.1. Platform Service – Identity Authentication Service	
12.	Aadhaar Vaulting Service	As per Section 3.2.2.2. Platform Service – Aadhaar Vaulting Service	
13.	SRN Vault	As per Section 3.2.2.3. Platform Service – SRN Vault	
14.	Seeding Validation Service	As per Section 3.2.2.4. Platform Service – Seeding Validation Service	
15.	Payment Disbursal Service	As per Section 3.2.2.5. Platform Service – Payment Disbursal Service	
16.	Payment Receipt Service	As per Section 3.2.2.6. Platform Service – Payment Receipt Service	
17.	Fetch Data Service	As per Section 3.2.2.7. Platform Service – Fetch Data Service	
18.	Push Data Service	As per Section 3.2.2.8. Platform Service – Push Data Service	
19.	Publish Document Service	As per Section 3.2.2.9. Platform Service – Publish Document Service	
20.	Anonymization and Deidentification Service	As per Section 3.2.2.10. Platform Service – Anonymization and Deidentification Service	
21.	Telemetry Service	As per Section 3.2.2.11. Platform Service – Telemetry Service	
22.	Feedback Service	As per Section 3.2.2.12. Platform Service – Feedback Service	
23.	Schedule Appointment Service	As per Section 3.2.2.13. Platform Service – Schedule Appointment Service	

Sl #	Components	Functional Specification	Compliance (Y/N – Page reference of data sheet/ proposal)
24.	Translation Service	As per Section 3.2.2.14. Platform Service – Translation Service	
25.	Messaging Service	As per Section 3.2.2.15. Platform Service – Messaging Service	
26.	Single Sign-On Service	As per Section 3.2.2.16. Platform Service – Single Sign-On Service	
27.	Data Sources (Social Registry)	As per Section 3.2.3. Data Sources (Social Registry)	
28.	Scheme Analysis and Policy Planning Tool	As per Section 3.2.1.1. Toolkits – Scheme Analysis and Policy Planning Tool	
29.	Data Collection Tool	As per Section 3.2.1.2. Toolkits – Data Collection Tool	
30.	Service Delivery Application	As per Section 3.2.1.3. Toolkits – Service Delivery Application	
31.	Grievance Management Tool	As per Section 3.2.1.4. Toolkits – Grievance Management Tool	
32.	Advanced Analytics Tool	As per Section 3.2.1.5. Toolkits – Advanced Analytics Tool	

6.3. Annexure-III: Minimum Technical Specifications

These are minimum technical specifications (but not exhaustive) to be complied by the bidders

Sl #	Components	Technical Specification	Compliance (Y/N) - Page reference of data sheet/ proposal
1.	IPeG Web Portal		
1.1.	IPeG Web Portal	Portal UI presentation layer: a. Defines the GUI and navigational flow of the application. b. End-users access to the GUI is through the browser. c. Format validation of data is entered in the GUI form. Interacts with the service layer that processes business logic.	
1.2.	IPeG Web Portal	The portal should not allow concurrent sessions for the same user. The system should automatically log a user out in case of session breakdowns (for e.g. communication failure, high inactivity period. These should be parameterized).	
1.3.	IPeG Web Portal	The portal should support workflow and rule engines using tools so that it can be integrated and configured.	
1.4.	IPeG Web Portal	The portal should have features and the capability to generate the e-forms that should have online and offline features. The portal should provide offline forms without any additional client software/tools or any additional browser plugins installed in the end user's machine. a. Forms can be customized and easily configured without making any changes in the backend system. b. Forms can be reused as a template to generate additional forms Forms can be saved while filling the information and submitted later.	
1.5.	IPeG Web Portal	Should have multilingual capability to be used in the web portal. The portal should be in English and Hindi and have capability to support other UTF-8 compliance languages	
1.6.	IPeG Web Portal	Transliteration capabilities to allow users to input data in one language (for e.g. English) and have the ability to transliterate the content to Hindi (required for IPEG records). Transliteration capabilities may also be used while generating any certificates etc.	
1.7.	IPeG Web Portal	The portal should implement security features, such as password complexity, automatic blocking (temporary/permanent) of user logins after a given number of unsuccessful login attempts (should be parameterized),	

Sl #	Components	Technical Specification	Compliance (Y/N) - Page reference of data sheet/ proposal
		controlled access to content stored on the portal and logging of security incidents.	
1.8.	IPeG Web Portal	The portal should provide a single sign-on functionality to access any module within the application with privilege rights based on the user profile using a single sign-on solution.	
1.9.	IPeG Web Portal	The portal should support HTTPS protocol on Secure Socket Layer (SSL).	
1.10.	IPeG Web Portal	The portal should support the leading browsers such as Internet Explorer, Firefox, Safari, Chrome etc.	
1.11.	IPeG Web Portal	The portal should be able to expose/publish functional applications seamlessly.	
1.12.	IPeG Web Portal	The portal should provide a search engine with advanced full-text search capabilities. The search engine should be able to search for requests within the portal.	
1.13.	IPeG Web Portal	Should provide support for comprehensive audit trail features such as: a. Daily activities log should be merged into the history log files. b. Date, time, and user-stamped transaction checklist should be generated for different transactions. c. All transaction screens should display system information. d. Daily activity reports should be provided to highlight all the transactions being processed during the day. Unsuccessful log-in attempts to the system should be recorded.	
1.14.	IPeG Web Portal	The portal should be compatible with popular mobile devices Operating systems (compatibility with iOS, Android Mobile) and should be device agnostic	
1.15.	IPeG Web Portal	The portal should be interoperable with industry standard databases.	
1.16.	IPeG Web Portal	Should authenticate users from Active Directory/LDAP, claim based authentication	
1.17.	IPeG Web Portal	Should support virtualization	
1.18.	IPeG Web Portal	The portal shall be accessible to all irrespective of technology, platform, devices or disabilities.	
1.19.	IPeG Web Portal	The portal shall adhere to the Web Content Accessibility Guidelines (WCAG 2.0), Guidelines for Indian Government Websites (GIGW) and W3C web content accessibility latest guidelines	
1.20.	IPeG Web Portal	Should support a broad range of standards, preferably open standards. Some examples are DOM 1.0, HTML 5, HTTP, HTTPS, MathML, ODBC, ODF (IS26300), Open XML (IS29500), OpenSearch, OpenType, PDF 1.7, PDF/A, RTF, RSS, ATOM, SOAP, SVG, REST, UDDI, Unicode, URI/URN, W3C XML Schema, and WCAG 2.0.	
1.21.	IPeG Web Portal	Should integrate with standard email services.	

Sl #	Components	Technical Specification	Compliance (Y/N) - Page reference of data sheet/ proposal
1.22.	IPeG Web Portal	Should integrate with instant messaging services.	
1.23.	IPeG Web Portal	The portal should implement basic design principles in portal design including use of consistent, unified common themes including a consistent unique stylesheet including fonts, colours, etc. and implement consistent look and feel and navigation.	
1.24.	IPeG Web Portal	Should support encryption and compression features.	
1.25.	IPeG Web Portal	Should support multiple roles with associated access controls.	
1.26.	IPeG Web Portal	Should support upload, store, organize and share documents.	
1.27.	IPeG Web Portal	Should provide multi-channel output capabilities.	
1.28.	IPeG Web Portal	The portal should have in-built security controls to protect against any malicious activity.	
1.29.	IPeG Web Portal	The portal should be capable of being deployed in high-availability and load balanced manners at both DC and DR hosted over cloud environment.	
1.30.	IPeG Web Portal	The portal should have a collaboration platform allowing content to be retrieved and worked on by a single or many authorized users. Changes should be tracked and authorized for publication or maybe ignored reverting to old versions. Other advanced forms of collaboration may allow multiple users to modify (or comment) a page at the same time in a collaboration session.	
1.31.	IPeG Web Portal	The portal should be compatible with structured and semi-structured sources.	
1.32.	IPeG Web Portal	Should provide rich text editor for content editing and a multiple file upload functionality.	
1.33.	IPeG Web Portal	Should have capability to add business validation rules	
2.	IPeG Mobile app		
2.1.	IPeG Mobile app	The mobile application should provide an intuitive and user-friendly GUI that enables users to navigate and apply actions with ease. The GUI should be responsive with very little or no delays or time lag at launch or whilst navigating through screens.	
2.2.	IPeG Mobile app	The mobile application should enable ease of configuration and changes to existing GUIs and support the introduction of new screens.	
2.3.	IPeG Mobile app	The mobile application should provide on screen tips and online help to aid users while interacting with it.	
2.4.	IPeG Mobile app	The mobile application should make use of data available in the existing database and reduce duplicate data entry	
2.5.	IPeG Mobile app	The mobile application should be easily customizable and easy to administer data in the database	
2.6.	IPeG Mobile app	Network level security and traffic should be encrypted using secured connectivity	
2.7.	IPeG Mobile app	The mobile application should structure overall content with proper tagging to make them screen reader friendly.	

Sl #	Components	Technical Specification	Compliance (Y/N) - Page reference of data sheet/ proposal
2.8.	IPeG Mobile app	The mobile application should ensure compatibility with latest versions of all major mobile operating systems i.e. Android and iOS.	
2.9.	IPeG Mobile app	The mobile application should develop resolution independent design structure i.e. should adjust itself automatically as per the screen resolution, form factor and size of the mobile	
2.10.	IPeG Mobile app	The mobile application should provide Role Based Access control	
2.11.	IPeG Mobile app	The mobile application should come with mobile threat prevention and recovery system	
2.12.	IPeG Mobile app	The mobile application should support both English and Hindi language	
2.13.	IPeG Mobile app	The mobile application shall be accessible to all irrespective of technology, platform, devices or disabilities.	
2.14.	IPeG Mobile app	There should be minimum use flash contents so that home page should be loaded quickly	
3.	Service Delivery Application		
3.1.	Service Delivery Application	Platform should allow configuration of the UI for both mobile and web application that works across mobile devices and web browsers respectively	
3.2.	Service Delivery Application	Web Application should be browser independent and can be accessed on Microsoft Edge, Google Chrome, Firefox and Safari.	
3.3.	Service Delivery Application	Platform should allow the development of applications from scratch or using a pre-defined template. The system should allow saving custom templates so that the end user can tailor a business process based on any of the custom templates.	
3.4.	Service Delivery Application	Application updates/upgrades should be available to the end-users without any down time	
3.5.	Service Delivery Application	Platform should be scalable for large set of concurrent users without need for any additional investment	
3.6.	Service Delivery Application	System shall facilitate re-engineering of processes and graphical process flow designer should support sequential process flows, parallel process flows, rule-based process flows and ad-hoc process flows	
3.7.	Service Delivery Application	Development Platform shall support Inbuilt web based Graphical workflow designer for modeling complex Business Processes using drag and drop facilities.	
3.8.	Service Delivery Application	The interface shall be easy to use so that Process owners can change the business process as and when required without any programming knowledge	
3.9.	Service Delivery Application	The system shall enable process designers to design multiple sub-processes. This includes mapping of the existing process instance to the newly created process instance as per mapping defined in the route	
3.10.	Service Delivery Application	Capability of form designer for creating responsive form to design forms that can be attached at one or more stages of workflow.	
3.11.	Service Delivery Application	Facility to define documents viewed and to be attached at individual stages.	
3.12.	Service Delivery Application	The system shall support better management of documents and store metadata information in primary database	

Sl #	Components	Technical Specification	Compliance (Y/N) - Page reference of data sheet/ proposal
3.13.	Service Delivery Application	The platform shall support the generation of statistical and management reports like: • Number of pending requests • Time taken to complete each task • User Performance Report • Average Process Time Report • Participant Report • Exception Details Report	
3.14.	Service Delivery Application	Should provide user specific/ role specific dashboard interface	
3.15.	Service Delivery Application	Facility to raise automatic exceptions on the basis of pre-defined conditions.	
4.	Advanced Analytics (may be utilized for Performance management & fraud detection)		
4.1.	Advanced Analytics	The proposed solution should provide Data Management, Data Quality, Analytics, Monitoring and Visualization capabilities	
4.2.	Advanced Analytics	The solution should be able to analyze Big Data and generate visualizations without any performance degradation	
4.3.	Advanced Analytics	The proposed solution should control access to applications, modules and functions based on user roles and privileges.	
4.4.	Advanced Analytics	The proposed solution should capture detailed auditing information related to key user activities within the system. Some key system actions may also be audited, for example automatic disposition of an alert. Audited actions should include (but are not limited to): • Login / logout • Performing a search (including details of the query and results if desired) • Viewing / editing • Deleting • Administration actions (i.e. changing configuration)	
4.5.	Advanced Analytics	The proposed solution should support data quality measurement	
4.6.	Advanced Analytics	The proposed solution should support data cleansing and de-duplication, duplicate suspect processing, house holding, with array of out-of-the- box standardization rules conform data to corporate standards – or can build customized rules for special situations	
4.7.	Advanced Analytics	Solution should generate code automatically from an intuitive, point-and-click interface so nontechnical users can profile, cleanse, blend and move data without specialized skills or training	
4.8.	Advanced Analytics	Solution should have inbuilt Data quality and Integration. It should Include prebuilt transformations and data cleansing functions to assist data scientists and business users in the exploration, refinement, and transformation of data analytical readiness.	
4.9.	Advanced Analytics	The solution should allow data load jobs to be scheduled to automate the process of loading data into memory	

Sl #	Components	Technical Specification	Compliance (Y/N) - Page reference of data sheet/ proposal
4.10.	Advanced Analytics	The solution should be cloud compliant and must provide cloud native capabilities like direct integration with CSP services	
4.11.	Advanced Analytics	The solution must support encryption of data in motion, between internal services and while fetching data from most sources	
4.12.	Advanced Analytics	The product must provide out of the box reporting & health checks	
4.13.	Advanced Analytics	Data Fetching and Updating – The solution would have facilities to fetch data from the required databases and get automatically updated without any assistance from the user. The frequency of the data updating will vary with the departments and would be decided by the Department.	
4.14.	Advanced Analytics	Geo-clustering and geo-querying capability to identify focus areas & areas that require improvement instantaneously	
4.15.	Advanced Analytics	The solution should provide following transformation nodes pre-built: - Clustering - Pattern Analysis - Basic Statistics - Frequency Distribution - Identification Analysis - Gender Analysis	
4.16.	Advanced Analytics	The proposed solution should provide fuzzy logic to induce tolerance during matching	
4.17.	Advanced Analytics	The proposed solution should have the capability to enrich data from internal data sources	
4.18.	Advanced Analytics	The proposed solution should have the capability to enrich data from internal/ external/third party data sources	
4.19.	Advanced Analytics	The proposed solution should have transformations to perform analytical operations like Correlations, Distribution Analysis, Frequency and Summarization.	
4.20.	Advanced Analytics	The proposed solution shall contain the data, software, processes needed to cleanse, consolidate and transform the data from their source system format to the data warehouse format.	
4.21.	Advanced Analytics	The proposed solution shall be able to check incoming data for quality, reliability, consistency and validity, and then transform as required.	
4.22.	Advanced Analytics	The proposed solution shall facilitate data profiling based on dynamic, user defined validation rules and support identification of user defined 'events' to trigger alerts (through email reports) to authorities	
4.23.	Advanced Analytics	The proposed solution Data Management should have capability of Interoperating with application integration technology in a single solution architecture, Supporting data integration across hybrid cloud and intercloud environments	
4.24.	Advanced Analytics	The proposed solution should support Nonrelational DBMS & relational DBMS integration	
4.25.	Advanced Analytics	The proposed solution shall have the capability to correct mistakes in spellings, inconsistencies, casings and abbreviations	
4.26.	Advanced Analytics	The proposed solution shall support correction logic for Indian names, addresses, phone numbers, pan numbers,	

Sl #	Components	Technical Specification	Compliance (Y/N) - Page reference of data sheet/ proposal
		passport number and other identification proof documents and demographic details	
4.27.	Advanced Analytics	The proposed solution shall support profile matching through multi-field text matching functionality on beneficiary -profile information (comparison could be on combination of name, PAN, address, telephone number etc.)	
4.28.	Advanced Analytics	The proposed solution should provide predictive modeling	
4.29.	Advanced Analytics	The proposed solution shall enable identification of cases for further Business Audit identified as a result of audit of alerted beneficiaries.	
4.30.	Advanced Analytics	The proposed solution should enable identification of suspicious beneficiary profiles through a judicious mix of anomaly detection, business rules, predictive modeling and network analytics	
4.31.	Advanced Analytics	The proposed solution should help analysts to visualize complex network of relationships between entities - such as people, places/ locations, things and events over time and across multiple dimensions	
4.32.	Advanced Analytics	The proposed solution should help analysts identify entity relationships that aren't obvious, traverse and query complex relationships, and uncover patterns and communities interactively	
4.33.	Advanced Analytics	The proposed solution should provide in-built features and advanced techniques for the analyst to detect rare events, anomalies and outliers and/or influence points to help determine, capture or remove them from downstream analysis	
4.34.	Advanced Analytics	The proposed solution should support Clustering of entities that are either user Defined or statistically chosen	
4.35.	Advanced Analytics	The proposed solution should support detection of patterns from the transaction data set over a defined time period for particular individuals / groups	
4.36.	Advanced Analytics	The proposed solution should have flexibility of high-performance imputation of missing values in features	
4.37.	Advanced Analytics	The proposed solution should be able to discover new patterns in the dataset (detect untrained patterns) and identify defined patterns in the dataset (trained patterns)	
4.38.	Advanced Analytics	The proposed solution should support processing, trend-analysis and modeling for prediction of data-points	
4.39.	Advanced Analytics	The proposed solution should support profile matching through user-defined (configurable) business rules through ad-hoc querying across multiple fields of entity-wise information from in-house and external agency data	
4.40.	Advanced Analytics	The proposed solution should have ability to identify beneficiaries with a malicious track record with respect to other schemes	
4.41.	Advanced Analytics	The proposed solution should have modern statistical, data mining and machine-learning techniques like: - Unsupervised and supervised learning algorithms, such as clustering, principal component analysis, linear and nonlinear regression, GLM, logistic regression, decision trees	

Sl #	Components	Technical Specification	Compliance (Y/N) - Page reference of data sheet/ proposal
4.42.	Advanced Analytics	The proposed solution should be open to coding language selection like python, R, Java	
4.43.	Advanced Analytics	Solution should be able to generate REST API in multiple languages like python for model consumption on new data	
4.44.	Advanced Analytics	The proposed solution shall allow identification of localities/ regions where high numbers of risky beneficiary profiles are detected.	
4.45.	Advanced Analytics	The proposed solution shall support ad-hoc querying of the voluminous transactional data such Registration Data, Approved profiles data, etc.	
4.46.	Advanced Analytics	The proposed solution shall support Time Series and scenario (“What-If”) analysis for dependent variables.	
4.47.	Advanced Analytics	The proposed solution shall generate periodic, beneficiary-wise, location-wise and scheme- wise analytical reports	
4.48.	Advanced Analytics	The solution should support containerized analytics like Docker that allows data scientists and analytical teams a flexible DevOps environment for working with containerized Analytics in the cloud.	
4.49.	Advanced Analytics	The solution should provide scaling of microservices related to underlying the model building engine.	
4.50.	Advanced Analytics	The proposed solution analytical reporting should allow 'On-the-fly' hierarchy creation for being able to traverse to lowest information to undertake root cause analysis	
4.51.	Advanced Analytics	The proposed solution analytical reporting shall have capability to generate analytical reports on the basis of top performers, worst performers scheme wise, department wise and district wise	
4.52.	Advanced Analytics	The solution should be capable of carrying out sentiment analysis determines whether a document has a positive sentiment, negative sentiment, or neutral sentiment based on the feeds/ data provided	
4.53.	Advanced Analytics	The proposed solution analytical reporting should support exploration of relationships (either transactional or demographic / profile based) of entities through appropriate visualization.	
4.54.	Advanced Analytics	The proposed solution analytical reporting shall have capability to generate MIS reports using GUI	
4.55.	Advanced Analytics	The proposed solution analytical reporting should have feature wherein Report can be drill down to most granular level of detail as their access controls / profiles allow	
4.56.	Advanced Analytics	The proposed solution analytical reporting should display trends within a dashboard	
4.57.	Advanced Analytics	The proposed solution analytical reporting should support Printing dashboard - Should allow printing of individual dashboards and email options	
4.58.	Advanced Analytics	The proposed solution Should support advanced analytics, statistical analysis, forecasting and advanced aggregation	
4.59.	Advanced Analytics	The proposed solution should provide facility to generate static or dynamic interactive visualization charts and graphs	
4.60.	Advanced Analytics	The proposed solution should have natural language processing capability such as text mining, search, categorization, summarization, entity and fact extraction	

Sl #	Components	Technical Specification	Compliance (Y/N) - Page reference of data sheet/ proposal
		which may be utilized for grievance management, fraud detection etc.	
4.61.	Advanced Analytics	The proposed solution should support English and Hindi language.	
5.	Key Technical Specifications of IPeG Platform Development		
5.1.	User Access and Security	Ability to create and define roles across the system/modules.	
5.2.	User Access and Security	Ability to define security against each role.	
5.3.	User Access and Security	Ability to create user groups.	
5.4.	User Access and Security	Ability to assign roles to user groups and/or users.	
5.5.	User Access and Security	Ability to assign users to user groups.	
5.6.	User Access and Security	Ability to create delegated security administrators.	
5.7.	User Access and Security	Ability to limit the delegated security administrators to manage security by: a. Users assigned to the delegated administrator b. Assign security for components/modules/forms that the delegated security administrator has been assigned to it c. Transaction level	
5.8.	User Access and Security	Ability to generate reports related to users and security. For e.g.: a. Full list of users b. Users based on selection criteria (selection by wildcard search on username, first name, last name, membership to user groups, assigned roles, etc.)	
5.9.	User Access and Security	Ability to provide automatic time out for entry transaction.	
5.10.	User Access and Security	Ability to provide automatic time out (log out) for user.	
5.11.	User Access and Security	Ability to support 2 factor authentications for users connecting to solutions from the internet.	
5.12.	User Access and Security	Centralized repository of all identification and access control data.	
5.13.	User Access and Security	Ability to provide or support single sign-on	
5.14.	User Access and Security	Ability to provide multiple roles for one user.	
5.15.	User Access and Security	Ability to support the remote operation of Security Management.	
5.16.	User Access and Security	Ability to support the remote operation of Diagnostic and Fine-tuning tools.	
5.17.	User Access and Security	Ability to provide time restriction on transactions.	
5.18.	User Access and Security	Ability to provide user login with time restriction.	
5.19.	User Access and Security	The system shall have a robust built-in security framework which covers the entire system/all its components.	
5.20.	User Access and Security	The system shall have a single security framework for all modules and components.	

Sl #	Components	Technical Specification	Compliance (Y/N) - Page reference of data sheet/ proposal
5.21.	User Access and Security	The system shall provide a unique user id and password to each user of the system	
5.22.	User Access and Security	The system shall deny access to all components / modules without this unique user id and password	
5.23.	User Access and Security	The system shall maintain a profile of each user consisting of one or more roles (role refers to the authority of each user to execute the tasks he / she performs)	
5.24.	User Access and Security	System shall allow administrators to manually lock accounts	
5.25.	Security Framework	The MSI shall ensure its developers are adequately trained in secure coding techniques, based on best practice guidance (i.e., the OWASP guide).	
5.26.	Security Framework	The MSI shall ensure that the concept of maker and checker is followed in order to prevent human error in all three phases of development, implementation and operation.	
5.27.	Security Framework	The MSI shall have a comprehensive documented secure development lifecycle system in place consistent with industry standard best practices including policies, training, audits, testing, emergency updates, proactive management and regular updates to the secure development lifecycle system itself.	
5.28.	Security Framework	The MSI shall follow Secure Application development guidelines of the CHIPS and the application shall be compliant with OWASP secure coding practices.	
5.29.	Security Framework	The MSI shall at all stages of development follow coding standards such as OWASP secure coding guidelines, W3C specifications etc. that support both writing secure code and the re-use of built-in security features and capabilities.	
5.30.	Security Framework	The MSI shall use a software version control system or repository.	
5.31.	Security Framework	The MSI shall ensure that system design is free from flaws that may lead to security breach.	
5.32.	Security Framework	All login pages shall contain captcha to ensure no brute force attempts could be attempted.	
5.33.	Security Framework	Two factor authentications based on OTP or soft token must be implemented on login pages, financial transactions, deleting functions, Admin logins etc. to ensure the second layer of authentication and authorization.	
5.34.	Security Framework	The MSI shall ensure that the development phase onwards following password policy is mandated in the application as well as management of the application as per ISO 27001 standard , CHIPS policy and procedure, and security best practices which include but not limited to : a. Password must be minimum 8 characters long b. Password must have at least one lowercase letter, one upper case letter, one special character, and one numerical digit c. Password must expire in 90 days d. Last three passwords shall not be allowed to be reused	

Sl #	Components	Technical Specification	Compliance (Y/N) - Page reference of data sheet/ proposal
5.35.	Security Framework	The application must have the capabilities to restrict files upload based on file type and file size. Although, the application should be able to detect the genuine file type (if get changed) and be able to protect against malicious imbedded payload.	
5.36.	Security Framework	Cryptography : a. The MSI shall ensure using the highest available public key exchange for encryption (PKI-2048 and AES-256 b. Input password must be hashed and salted before being transmitted across to application server from both external and internal domains. (SHA 256/512 shall be used to hashing) Pseudorandom values must be used wherever application such in case of generation of salt for password, session tokens, etc.	
5.37.	Security Framework	The MSI shall ensure that the test environments emulate the production environment as closely as possible.	
5.38.	Security Framework	The MSI shall use secure configuration options for supporting technology, libraries, packages and tools.	
5.39.	Security Framework	The MSI shall deploy test and production applications from the version control system or repository.	
5.40.	Security Framework	The MSI shall tag/label versions so that they can be extracted at a later time.	
5.41.	Security Framework	The MSI shall ensure that all new or modified software, including the application of patches, is adequately tested, approved, and consistent with the change and management standards before deployment.	
5.42.	Security Framework	The MSI shall also develop a disaster recovery plan for restoration of the applications developed in the event of a disaster or major incident.	
5.43.	Security Framework	The MSI shall ensure that the production, test, and development environments are physically separated.	
5.44.	Security Framework	Updates/ Upgrades/ New releases/ New versions/ Patches/ Bug fixes: The MSI shall provide from time to time the Updates/ Upgrades/ New releases/ New versions/ Patches/ Bug fixes of the applications as required. The MSI shall provide free Updates/ Upgrades/ New releases/ New versions/ Patches/ Bug fixes of the software/libraries etc. as and when released.	
5.45.	Security Framework	The MSI shall ensure that updates to operational software, applications and program libraries are performed by designated, trained personnel.	

Sl #	Components	Technical Specification	Compliance (Y/N) - Page reference of data sheet/ proposal
5.46.	Security Framework	The MSI shall identify minimum security training requirements and provide minimum security training to staff that access information systems.	
5.47.	Security Framework	All deletions shall be soft deletes in which the "deleted" objects are either logically marked as deleted or are moved to an online archive.	
5.48.	Security Framework	The Application shall maintain data for at least as long as the data retention policy requirements (may be 10 years) of the underlying records. And must allow CHIPS to enforce data retention policy.	
5.49.	Authentication & authorization	The MSI shall ensure that the solution developed have appropriate authentication mechanisms in place. Application user authentication & authorization related transactions shall be encrypted.	
5.50.	Authentication & authorization	The MSI shall ensure that the applications developed must perform authorization checks before performing any action that creates, views, updates, transmits or deletes Confidential Information. Authorization logic must be highly configurable and alterable without code changes. Authorization checks must verify the user has appropriate role to perform the requested action, and also the correct scope.	
5.51.	Authentication & authorization	The MSI shall at the minimum implement Authentication, Authorization and Access Control as included in OWASP Secure Coding Practices v2 (https://www.owasp.org/images/0/08/OWASP_SCP_Quick_Reference_Guide_v2.pdf)	
5.52.	Authentication & authorization	Any access to end users to database shall only be via application.	
5.53.	Authentication & authorization	The system should support multi- factor authentication. Bidder to propose the approach.	
5.54.	Authentication & authorization	The system shall have the capability to control access based on time for certain roles (e.g., certain users can log in to the system during office hours only).	
5.55.	Authentication & authorization	The system shall have a maximum number of login attempts where the maximum number is configurable.	
5.56.	Authentication & authorization	Provide power users with the capability of assigning authority to other users within their department.	
5.57.	Authentication & authorization	Provide the super users with the ability to create a Segregation of Duty (SOD) matrix within the system.	

Sl #	Components	Technical Specification	Compliance (Y/N) - Page reference of data sheet/ proposal
5.58.	Authentication & authorization	The system should have two different login portals for internal and external users	
5.59.	Authentication & authorization	The MSI shall ensure that the solution allows a user to access various functions, forms, screens, sub modules, information, etc. as per the authorization and user role permitted by the system administrator as per available guidelines and policies.	
5.60.	Authentication & authorization	The MSI shall configure the version control system or repository to prevent and detect unauthorized changes.	
5.61.	Authentication & authorization	The MSI shall ensure that only authorized release managers and system administrators have access to the production environment where the production executable code for an application resides.	
5.62.	Authentication & authorization	The MSI shall provide a self-compliance certificate of the applications/portals developed covering at the minimum assessment of authentication mechanism provided in the application /components/modules	
5.63.	Authentication & authorization	The MSI shall ensure that all access logs are being recorded for the activates performed by the users .	
5.64.	Authentication & authorization	Proper audit logs shall be stored for application activities performed by users.	
5.65.	Authentication & authorization	Audit logs shall be stored and maintained for the changes done by MSI in the application.	
5.66.	Authentication & authorization	Alerts and notifications for taxpayers through SMS or email for any system transaction to be aware if the account get compromised.	
5.67.	Authentication & authorization	The MSI shall ensure that federated identify and access management is implemented in application	
5.68.	Logging & Monitoring	The AP shall ensure that event logging creates an accurate record of user activity such as which users accessed which system and for how long. The applications shall log all types of events especially those related to security. All the activities by management users, internal and external users shall be recorded with timestamp, source IP, other source details such as browsers, user, machine name, hardware address etc.	
5.69.	Logging & Monitoring	The MSI shall ensure response actions to incidents that might affect confidential information or systems are conducted quickly and with ample resources.	

Sl #	Components	Technical Specification	Compliance (Y/N) - Page reference of data sheet/ proposal
5.70.	Logging & Monitoring	The MSI shall report security incidents that occur on the information systems that may affect application or any connected systems within 24 hours of discovery.	
5.71.	Logging & Monitoring	The MSI shall ensure in terms of logging for database that it is capable of generating audit trails which include details such as who inserted, changed, or deleted the data, the prior value, the new value, the type of change (insert, delete, or update), the date and time of the change as well as a reference to the record being changed (a snapshot before and after the change) for all system and database actions.	
5.72.	Logging & Monitoring	Audit trail shall be stored, and no access should be allowed to any of the user roles to make changes to audit trail.	
5.73.	Logging & Monitoring	Application shall have the capability to print or export the audit trail for actions or investigations.	
5.74.	Logging & Monitoring	Application shall ensure that audit trail records are maintained for at least as long as the retention of the underlying records.	
5.75.	Logging & Monitoring	Application shall allow logging and reviewing of all system administrators and users actions.	
5.76.	Logging & Monitoring	Application shall record and alert the attempts to change the master data or system configuration.	
5.77.	Logging & Monitoring	Application shall be able to maintain an audit log that can be turned on and off and will be configured to the object level, table level and column level	
5.78.	Logging & Monitoring	Application shall be able to mask specific data or object for all system users (business users, system administrators, system operators, Database administrators, etc.)	
5.79.	Logging & Monitoring	Application shall be able to control access to audit logs and audit trails.	
5.80.	Logging & Monitoring	The solution shall ensure logs including at least the following: a. Authentication and authorization events – logging in, logging out, failed logins. These shall include date/time, success/failure, resources being authorized, the user requesting the authorization and the IP address or location of the authentication attempt b. Logs for deletion of any data c. Logs of all administrator activity d. Logs of modification to data characteristics: permissions, location and field type e. Logs for all user activities	

Sl #	Components	Technical Specification	Compliance (Y/N) - Page reference of data sheet/ proposal
5.81.	Logging & Monitoring	It shall be ensured by the MSI that respective alerts are configured in SIEM related to critical changes in application. The MSI shall assist in creating use case on SIEM covering changes done on user accounts ,changes in database, login failure, admin activity as per the CHIPS requirements.	
5.82.	Application Security	The MSI shall develop process and plans to update the application to stay current with platforms and infrastructure.	
5.83.	Application Security	The MSI shall use commercially reasonable efforts to secure and defend any System housing Confidential Information against third parties who may seek to breach the security thereof, including, but not limited to breaches by unauthorized access or making unauthorized modifications to such System.	
5.84.	Application Security	The MSI shall engage an independent third party annually to assess the practical security of applications. These reviews must include penetration tests from the perspective of an external attacker and an internal user with common privileges. The penetration tests must include all systems exposed to the internet and any systems, internal or external, that handle confidential information.	
5.85.	Application Security	The CHIPS may obtain periodic integrity & compliance statements, for application and related infrastructure components used by the MSI, in writing from the selected MSI providing for reasonable level of assurance about the applications being free of malware & viruses, free of any obvious bugs, free of any covert channels in the code, and free of any known vulnerabilities.	
5.86.	Application Security	The MSI shall perform a vulnerability scan of the entire solution and appropriately remediate findings based on risk before placing the solution into production.	
5.87.	Application Security	The MSI shall review and test all application code for security weaknesses and backdoors prior to deployment within CHIPS. All high-risk findings and exploitable vulnerabilities must be resolved before the Application is released. A development manager of MSI must certify in writing to the CHIPS that a security review has been conducted and that all risks are acceptable before every release.	
5.88.	Application Security	The MSI shall ensure that all significant modifications, major enhancements, and new systems undergo system testing prior to installation of the software in production.	
5.89.	Application Security	The MSI shall certify and complete continuity planning according to the CHIPS security requirements before moving information systems into a production status.	
5.90.	Application Security	The MSI shall provide a self-compliance certificate of the applications/portals developed covering at the minimum OWASP Top 10 Vulnerability assessment report of the applications/portals developed.	
5.91.	Application Security	Independent security assessments (Gray Box, White Box and VMSIT) shall be performed for the web application(s) and mobile application along with its related infrastructure	

Sl #	Components	Technical Specification	Compliance (Y/N) - Page reference of data sheet/ proposal
		components (collectively referred as 'Information Processing Facility'), designed/ developed for [the CHIPS] by the MSI.	
5.92.	Application Security	The MSI shall perform a vulnerability scan of the entire solution and appropriately remediate findings based on risk before placing the solution into production.	
5.93.	Application Security	The MSI shall ensure that all data input fields properly validate the input in order to minimize the threat of cross site scripting and SQL injection.	
5.94.	Application Security	The MSI shall at the minimum implement Data and Input validation for all kind of input data, parameterized database querying, error handling, logging and include secure coding practices as included in OWASP Secure Coding Practices v2 (https://www.owasp.org/images/0/08/OWASP_SCP_Quick_Reference_Guide_v2.pdf)	
5.95.	Application Security	The MSI shall ensure that the application and API does not use components with known vulnerabilities. The MSI shall remove unused dependencies, unnecessary features, components, files etc. and continuously check code dependencies for detecting known vulnerabilities.	
5.96.	Application Security	Secure coding guidelines shall be followed. Secure coding guidelines shall include controls against SQL injection, command injection, input validation, cross site scripting, directory traversal, buffer overflows, resource exhaustion attacks etc. OWASP Top 10 standard shall be mapped in the secure coding guidelines to cover all major vulnerabilities.	
5.97.	Application Security	Validation checks shall be incorporated into the application to detect any corruption of information through processing errors or deliberate acts.	
5.98.	Application Security	Data output from an application shall be validated to ensure that the processing of stored information is correct and appropriate to the circumstances.	
5.99.	Application Security	Shall implement secure error handling practices in the application.	
5.100.	Application Security	The MSI shall comply with CHIPS's IT security standards, policy and procedures.	
5.101.	Application Security	Generate Log and allow review of all remote connection activity (e.g. firewall, VPN connection, dial-up etc.).	
5.102.	Data Privacy, Integrity and Confidentiality	The MSI shall ensure that the data transferred across network shall be encrypted using Public Key (PKI) Infrastructure and complete end point data protection shall be provided at client site such that any type of data pilferage using unauthorized copying, storing and emailing could be prohibited.	
5.103.	Data Privacy, Integrity and Confidentiality	The MSI shall choose keys randomly from the entire key space and ensure that encryption keys allow for retrieval for administrative or forensic use.	
5.104.	Data Privacy, Integrity and Confidentiality	The MSI shall ensure to protect documents by assigning security parameters and criteria in order to provide more effective protection for an electronic document in order to maintain Confidentiality, Authorization, Accountability, Integrity, Authenticity and Non-repudiation.	
5.105.	Data Privacy, Integrity and Confidentiality	The MSI shall provide a self-compliance certificate of the applications/portals developed covering at the minimum	

Sl #	Components	Technical Specification	Compliance (Y/N) - Page reference of data sheet/ proposal
		assessment of data encryption mechanisms implemented for the solution	
5.106.	Data Privacy, Integrity and Confidentiality	Implementation team shall ensure that data integrity checks are enabled for data exchange	
5.107.	Data Privacy, Integrity and Confidentiality	The MSI shall implement data encryption for the data in exchange and data at rest.	
5.108.	Data Privacy, Integrity and Confidentiality	Relevant international standard such as General Data Protection Regulations GDPR are followed. This should include 1. Asking for consent from the user before data collection and processing 2. Data should be stored anonymously 3. User should be informed if their data is breached Application should facilitate deletion of data related to personal information of a user, if explicitly requested by the user.	
5.109.	Data Privacy, Integrity and Confidentiality	The MSI shall ensure that the appropriate security model is selected for development of application.	
5.110.	Data Privacy, Integrity and Confidentiality	The MSI shall also ensure that Secure development life cycle SDLC is followed in development embedding GDPR into the SDLC .	
5.111.	Data at Rest	The MSI shall provide a self-compliance certificate of the applications/portals developed covering at the minimum assessment of data access privileges, retention periods and archival mechanisms.	
5.112.	Data at Rest	The MSI shall ensure that the data at rest that is stored outside of hardened application or database production systems is protected by encryption consistent with NIST/SANS/OWASP and CHIPS's recommendations.	
5.113.	Data at Rest	The MSI shall ensure all mobile applications shall be designed and developed in a way that it ensures security of the application and data on the device.	
5.114.	Data Encryption & Object Signing	All the interfaces between various applications and user are encrypted using appropriate protocols (such as HTTPS, IPSec, SSL etc.), algorithm and key pairs.	
5.115.	Data Encryption & Object Signing	System shall support 128/256/512 bit encryption for transmission of the data over the Internet.	
5.116.	Data Encryption & Object Signing	Object signing and encryption of attachments (documents) shall be compliant to published govt standards.	
5.117.	Data Encryption & Object Signing	Proposed solution shall be secured to both internal and external parties (such as through encryption)	
5.118.	Data Encryption & Object Signing	The Network/Transport level shall include Network Link Encryption (IPSEC) and encrypted HTTP session using TLS/SSL (HTTPS)	
5.119.	Data Encryption & Object Signing	Business data shall be encrypted in the database and DBA shall not be able to read or modify it.	

Sl #	Components	Technical Specification	Compliance (Y/N) - Page reference of data sheet/ proposal
5.120.	Data Encryption & Object Signing	Audit controls, electronic signatures, data encryption and other methods shall be used to assure the authenticity of transaction and other relevant data	
5.121.	Data Encryption & Object Signing	Following events shall be considered as security incidents: unsuccessful log-on, intrusion detection, malfunctioning of encryption facility, etc.	
5.122.	Data Encryption & Object Signing	Shall develop a procedure for archiving the log files and ensure security of the log files.	
5.123.	Data Encryption & Object Signing	A separate environment shall be maintained for production, test and development to reduce the risks of unauthorized access or changes.	
5.124.	Data Encryption & Object Signing	The system shall have the functionality to record all the administrator and user level activities including the failed attempts.	
5.125.	Data Encryption & Object Signing	Shall protect logging facilities and log information against tampering and unauthorized access.	
5.126.	Data Encryption & Object Signing	Information security baseline document shall be developed for all the infrastructure components such as database, operating system, router, switch etc. based on industry best practices guidelines.	
5.127.	Data Encryption & Object Signing	Provisions shall be made for secure content management.	
5.128.	API Security	Applications and interfaces (APIs) shall be designed, developed, and deployed in accordance with industry acceptable standards (e.g., OWASP, ISO 27001 etc.) and adhere to applicable legal, statutory, or regulatory compliance obligations of the CHIPS.	
5.129.	API Security	The MSI shall develop APIs which use secure authentication methods such as OAuth, Two factor authentication, content-based access control, etc. In order to prevent exchange of malicious data between application and API, validation could be performed using time-based API access token which can further be validated using OTP and identity token before interacting with the application. This token should be a pseudo random token generated uniquely on each request.	
5.130.	API Security	The MSI shall implement security measures which protect APIs from malicious data, improper requests, and denial of service attacks. Any request must be validated for authentication and authorization based on user requesting the data. The MSI shall implement strong cipher suit and use TLS 1.2 or above cryptographic protocols for exchange of information.	
5.131.	API Security	The MSI shall ensure that the API endpoints are secure and that the API is thoroughly tested for OWASP Top 10 issues. API should not expose any information in URL, proper input validation needs to be implemented etc.	
5.132.	API Security	The MSI provider shall implement security measures such as data validation and rate limiting, force encryption and validate user-submitted content interacting with the CHIPS applications.	

Sl #	Components	Technical Specification	Compliance (Y/N) - Page reference of data sheet/ proposal
5.133.	API Security	The MSI shall ensure that the API developed does not use components with known vulnerabilities. The MSI shall remove unused dependencies, unnecessary features, components, files, etc. and continuously check code dependencies for detecting known vulnerabilities.	
5.134.	API Security	For proper logging all the API request must be sent with related timestamps.	
5.135.	API Security	The MSI shall implement adequate auditing and logging mechanisms to ensure that all login, access control failures, and server-side input validation failures are logged with enough user context to identify suspicious or malicious activities.	
5.136.	Containerization	Proposed container platform would support a secure, enterprise-grade orchestration that provides policy-based control and automation for applications. Cluster services, scheduling, and orchestration provide load-balancing and auto-scaling capabilities should be available	
5.137.	Containerization	The platform would have capability to run both stateful and stateless applications.	
5.138.	Containerization	The container platform would support deployment and orchestration of multiple containers formats (for e.g. docker etc.) for preventing any technology lock in.	
5.139.	Containerization	The platform would have inbuilt management and monitoring capabilities.	
5.140.	Containerization	The platform would have automated application build capability – from source code to a runnable container image.	
5.141.	Containerization	The platform would have / support integration with CI / CD tools. Integrated CI / CD tools has to be part of solution.	
5.142.	Containerization	The platform would support multiple technologies as runtime platforms for applications such as – Java, PHP, Python, Ruby, Perl, Node.js etc.	
5.143.	Containerization	The platform would provide auto scaling capability for automatically running appropriate number of container instances as per load requirements.	
5.144.	Containerization	The platform would provide container instance auto healing capability.	
5.145.	Containerization	The platform would provide application / container version management, auto build of new application container instance in test environment basis on application code new version commit. Roll back to earlier version.	
5.146.	Containerization	The platform would provide deployment strategies support such as for ensuring no/minimum downtime for application updates / upgrades.	
5.147.	Containerization	The platform would provide centralized logging capability (including applications logs from container instances) for audit, logs analysis & ease of management purpose.	
5.148.	Containerization	The platform would provide integrated container native persistent storage capabilities.	
5.149.	Distributed Caching & messaging	Application development should involve distributed caching & distributed messaging	
5.150.	Testing Tools	MSI must implement and utilize throughout the project, automated testing tool and performance and load testing tools before very release as applicable	

OEM Criteria Compliance

Sl #	Components	Criteria	Supporting Documents Required	Compliance Y/N - Page reference of data sheet/ proposal

1.	Advanced Analytics Tool	• The bidder's proposed advanced analytics solution shall be successfully installed and configured in three different Government Organizations
		• The proposed OEM solution should appear in either of the below three-
		  ○ latest Gartner's Leaders Quadrant (Data Science and Machine Learning Platforms)
		  ○ latest Forrester Wave Leaders wave (Multimodal Predictive Analytics and Machine Learning)
		  ○ latest IDC's Worldwide Advanced Machine Learning Software Platforms Leaders
		• It should support programming from popular open source languages.
		• The bidder's proposed advanced analytics solution should be configurable/ customizable Commercial off The Shelf (COTS) with the requirements of the department to reduce implementation efforts, time and cost
		• The bidder's proposed advanced analytics solution should support migration from on-premise to/ on alternate MeitY approved cloud offerings for future readiness and vice versa, to enable successful deployment and running of the solution on any environment platform.
		• The proposed solution should provide perpetual licenses
			• OEM need to provide relevant Purchase order / licence agreement documents as proof.
			• Latest respective reports from Gartner/ Forrester/ IDC to be provided.	

2.	Service Delivery Application	• The bidder's proposed solution shall be successfully installed and configured in at least one Government Organizations. • The proposed solution should appear in any Quadrant of Gartner's Magic Quadrant for Enterprise Low-Code Application Platforms • The proposed solution should provide perpetual licenses	OEM need to provide relevant Purchase order / licence agreement documents as proof.	
3.	Cloud service provider	• Should be a MeitY empanelled Cloud Service Providers. • The bidder's proposed CSP must have provided cloud hosting services in minimum three projects at State Government / Central Governments/ PSUs with a minimum value of cloud hosting services more than 2 Cr. Across these three projects in last three years.	Documentary proof to be provided.	

6.4. Annexure–IV: List of tentative data fields in Social Registry

S. No.	Data Field for Social Registry – Central Part (Illustrative)
1	Social Registry Number (SRN)
2	Name
3	Father/Husband Name
4	Ration Card Family Number
5	Ration Card Member Number
6	Gender
7	Date of Birth
8	Mobile Number
9	Email Address
10	Bank Account Number
11	IFSC Code
12	**Communication Address**
A	House/Building/Apartment Number
B	Street/Road/Lane
C	Landmark
D	Area/Locality/Sector
E	Village/ Town/ City
F	Sub-District Code
G	District Code
H	State Code
I	Pin Code
13	**Location Address**
A	Urban / Rural
B	Urban Local Body / Gram Panchayat
C	Ward / Village

6.5. Annexure–V: Study of first 5 public services

1. Merit Scholarship [Department of Technical Education];
2. Samajik Suraksha Pension Scheme [Department of Social Welfare];
3. Post-Matric Scholarship Scheme for OBC students [Tribal Department];
4. Bhagini Prasooti Sahayata Yojana [Labor Department]; and
5. Navnihaal Chhatravritti Yojana [Labor Department].

6.6. Annexure–VI: List of remaining public services out of which 45 will be selected based on department's adoption and business case priority

SNo.	Name of the implementing Ministry/Department	Scheme Name	Category	Benefit Type
1	Department of Agriculture and Biotechnology	Agriculture Technical Management Agency (ATMA) - Extension Functionaries	Centrally Sponsored	Cash
2	Department of Agriculture and Biotechnology	Agriculture Technical Management Agency (ATMA) - Farmers	Centrally Sponsored	Cash
3	Department of Agriculture and Biotechnology	Livestock Health and Diseases Control	Centrally Sponsored	In Kind
4	Department of Agriculture and Biotechnology	Mission for Integrated Horticulture Development (MIDH)	Centrally Sponsored	Cash
5	Department of Agriculture and Biotechnology	National Food Security Mission	Centrally Sponsored	In Kind
6	Department of Agriculture and Biotechnology	Pradhan Mantri Kirshi Sinchai Yojana - Horticulture	Centrally Sponsored	Cash
7	Department of Agriculture and Biotechnology	Pradhan Mantri Krishi Sinchai Yojana - Agriculture	Centrally Sponsored	In Kind
8	Department of Agriculture and Biotechnology	Sub Mission on Agriculture Mechanization	Centrally Sponsored	Cash
9	Department of Agriculture and Biotechnology	Sub-Mission on Seeds and Planting Material	Centrally Sponsored	Cash
10	Department of Agriculture and Biotechnology	Sub Mission on Agroforestry	Centrally Sponsored	Cash & In Kind
11	Department of Fisheries	Development of Inland Fisheries and Aquaculture	Centrally Sponsored	Cash
12	Department of Fisheries	Development of Marine Fisheries, Infrastructure and Post-Harvest Operation	Centrally Sponsored	Cash
13	Department of Fisheries	Scheme for welfare of fishermen	Centrally Sponsored	Cash
14	Department of Health and Family Welfare	Ayushman Bharat - Pradhan Mantri Jan Arogya Yojana (AB-PMJAY)	Centrally Sponsored	In Kind
15	Department of Health and Family Welfare	NIKSHAY - TB patient incentive for nutritional support	Centrally Sponsored	Cash & In Kind
16	Department of School Education	Pre Matric Scholarship for Scheduled Caste Students studying in classes IX and X	Centrally Sponsored	Cash
17	Department of School Education	Inclusive Education for Disabled at Secondary Stage	Centrally Sponsored	Cash
18	Department of School Education	Kind benefit under IEDSS of RMSA	Centrally Sponsored	Cash
19	Department of School Education	Merit cum Means scholarship - School	Centrally Sponsored	Cash

SNo.	Name of the implementing Ministry/Department	Scheme Name	Category	Benefit Type
20	Department of School Education	Mid-Day Meal Scheme	Centrally Sponsored	In Kind
21	Department of School Education	National Scheme of Incentive to Girls for Secondary Education	Centrally Sponsored	Cash
22	Department of School Education	Post-Matric Scholarship to the SC Students studying in classes XI and XII	Centrally Sponsored	Cash
23	Department of School Education	Post-Matric Scholarship to the ST Students studying in classes XI and XII	Centrally Sponsored	Cash
24	Department of School Education	Pre-Matric Scholarship to the OBC Students studying in classes IX and X	Centrally Sponsored	Cash
25	Department of School Education	Pre-Matric Scholarship to the ST Students studying in classes IX and X	Centrally Sponsored	Cash
26	Department of School Education	Sarva Shiksha Abhiyan - Free Textbook	Centrally Sponsored	In Kind
27	Department of School Education	Sarva Shiksha Abhiyan - Free Uniform	Centrally Sponsored	In Kind
28	Department of School Education	Scheme For Providing Quality Education In Madrasa (SPQEM)	Centrally Sponsored	Cash & In Kind
29	Department of Social Welfare	Centrally Sponsored Scheme of Dr.Ambedkar Pre-Matric and Post-Matric Scholarship for DNTs	Centrally Sponsored	Cash
30	Department of Social Welfare	Centrally Sponsored Scheme of Post-Matric Scholarship for OBC Students for studying in India	Centrally Sponsored	Cash
31	Department of Social Welfare	National Family Benefit Scheme	Centrally Sponsored	Cash
32	Department of Social Welfare	Pre-Matric Scholarships to the Children of those Engaged in occupations involving cleaning and prone to health hazards	Centrally Sponsored	Cash
33	Department of Technical Education	Pradhan Mantri Kaushal Vikas Yojana Component II	Centrally Sponsored	Cash
34	Department Of Tribal Affairs	Vocational Training Centres in Tribal Areas	Centrally Sponsored	Cash & In Kind
35	Department of Women and Child Development	Child Protection Services - Facilities to Beneficiaries	Centrally Sponsored	In Kind
36	Department of Women and Child Development	Child Protection Services - Facilities to Beneficiaries (Sponsorship)	Centrally Sponsored	Cash
37	Department of Women and Child Development	Integrated Child Development Services - Supplementary Nutrition	Centrally Sponsored	In Kind
38	Department of Women and Child Development	Integrated Child Development Services - Training	Centrally Sponsored	In Kind

SNo.	Name of the implementing Ministry/Department	Scheme Name	Category	Benefit Type
39	Department of Women and Child Development	Integrated Child Development Services -Honrorarium to AWW and AWH	Centrally Sponsored	Cash
40	Department of Women and Child Development	Integrated Child Protection Scheme-Salary of staff	Centrally Sponsored	Cash
41	Department of Women and Child Development	National Creche Scheme-Honorarium to Workers	Centrally Sponsored	Cash
42	Department of Women and Child Development	National Creche Scheme-Nutrition	Centrally Sponsored	In Kind
43	Department of Women and Child Development	One Stop Centre - Payment of Salary of Staff	Centrally Sponsored	Cash
44	Department of Women and Child Development	Pradhan Mantri Matru Vandana Yojana	Centrally Sponsored	Cash
45	Department of Women and Child Development	Protection and Empowerment of Women Swdhar Greh-support to training cum employment program	Centrally Sponsored	Cash & In Kind
46	Department of Women and Child Development	Protection and Empowerment of Women- National Mission for Empowerment of Women	Centrally Sponsored	In Kind
47	Department of Women and Child Development	Protection and Empowerment of Women-Comprehensive Scheme for combating Trafficking of Women and Children-Ujjawla-Salary	Centrally Sponsored	Cash
48	Department of Women and Child Development	Protection and Empowerment of Women-Comprehensive Scheme for combating Trafficking of Women and Children-Ujjawla-Facilities to beneficiaries	Centrally Sponsored	Cash
49	Department of Women and Child Development	Protection and Empowerment of Women-Swdhar Greh- Salary to staff	Centrally Sponsored	Cash
50	Department of Women and Child Development	Protection and Empowerment of Women-Swdhar Greh-facilities to beneficiaries	Centrally Sponsored	In Kind
51	Department of Women and Child Development	Scheme For Adolescent Girls	Centrally Sponsored	Cash
52	Forest Department	Integrated Development of Wild Life Habitats	Centrally Sponsored	Cash
53	Forest Department	Achanakmar Amarkantak Biosphere Reserve Development	Centrally Sponsored	Cash
54	Forest Department	Green India Mission National Afforestation Programme	Centrally Sponsored	Cash & In Kind
55	Forest Department	Project Elephant	Centrally Sponsored	Cash
56	Forest Department	Project Tiger	Centrally Sponsored	Cash

SNo.	Name of the implementing Ministry/Department	Scheme Name	Category	Benefit Type
57	Panchayat and Rural Development Department	DDUGKY	Centrally Sponsored	In Kind
58	Panchayat and Rural Development Department	MGNREGS	Centrally Sponsored	Cash
59	Panchayat and Rural Development Department	National Rural Livelihoods Mission	Centrally Sponsored	Cash & In Kind
60	Panchayat and Rural Development Department	PMAY Grameen	Centrally Sponsored	Cash
61	Panchayat and Rural Development Department	SWACHH BHARAT MISSION GRAMEEN	Centrally Sponsored	Cash
62	Public Health and Family Welfare Department	ASHA Incentive	Centrally Sponsored	Cash
63	Public Health and Family Welfare Department	Family Planning Compensation schemes	Centrally Sponsored	Cash
64	Public Health and Family Welfare Department	Janani Shishu Suraksha Karyakram	Centrally Sponsored	Cash
65	Public Health and Family Welfare Department	Janani Suraksha Yojana	Centrally Sponsored	Cash
66	Public Health and Family Welfare Department	National Ayush Mission	Centrally Sponsored	In Kind
67	Public Health and Family Welfare Department	NIKSHAY - DOT Provider Honorarium	Centrally Sponsored	Cash
68	Public Health and Family Welfare Department	NIKSHAY - TB Notification incentive for Private Sector	Centrally Sponsored	Cash
69	Public Health and Family Welfare Department	Nikshay - Tribal TB patients	Centrally Sponsored	Cash
70	Public Health and Family Welfare Department	Payments to contractual staff	Centrally Sponsored	Cash
71	Social Welfare Department	Indira Gandhi National Disability Pension Scheme	Centrally Sponsored	Cash
72	Social Welfare Department	Indira Gandhi National Old Age Pension Scheme	Centrally Sponsored	Cash
73	Social Welfare Department	Indira Gandhi National Widow Pension Scheme	Centrally Sponsored	Cash
74	Tribal Department	Centrally Sponsored Scheme For Implementation Of Protection Of Civil Rights Act 1955 And Scheduled Castes And Scheduled Castes And Scheduled Tribes (Prevention Of Atrocities Act, 1989)	Centrally Sponsored	Cash
75	Tribal Department	Dr. Ambedkar Centrally Sponsored Scheme Of Post-Matric Scholarships For The Economically Backward Class (EBC) Students	Centrally Sponsored	Cash
76	Tribal Department	Post-Matric Scholarship Scheme for SC students	Centrally Sponsored	Cash

SNo.	Name of the implementing Ministry/Department	Scheme Name	Category	Benefit Type
77	Tribal Department	Post-Matric Scholarship Scheme for ST students	Centrally Sponsored	Cash
78	Tribal Department	Scheme of Development of Particularly Vulnerable Tribal Groups	Centrally Sponsored	Cash
79	Urban Administration and Development Department	DAY-NULM (ESTP)	Centrally Sponsored	In Kind
80	Urban Administration and Development Department	DAY-NULM (Sangwari)	Centrally Sponsored	Cash
81	Urban Administration and Development Department	DAY-NULM (SEP)	Centrally Sponsored	Cash
82	Urban Administration and Development Department	DAY-NULM (SMID)	Centrally Sponsored	Cash
83	Urban Administration and Development Department	PRADHAN MANTRI AWAAS YOJANA URBAN, BLC	Centrally Sponsored	Cash
84	Urban Administration and Development Department	PRADHAN MANTRI AWAAS YOJANA URBAN, PPP	Centrally Sponsored	In Kind
85	Urban Administration and Development Department	PRADHAN MANTRI AWAAS YOJANA URBAN- AHP	Centrally Sponsored	In Kind
86	Urban Administration and Development Department	SWACHH BHARAT MISSION URBAN - IHHL	Centrally Sponsored	Cash
87	Cooperative Department	Sahkari Samitiyon me SC evam ST varg ke sadasya banane ke liye Aansha Kray Hetu Anudan	State/UTs Scheme	Cash
88	Department of Agriculture and Biotechnology	Buck distribution scheme	State/UTs Scheme	In Kind
89	Department of Agriculture and Biotechnology	Dalhan Utpadan Pratyahan Yojana	State/UTs Scheme	Cash & In Kind
90	Department of Agriculture and Biotechnology	Fasal Pradarshan Yojana	State/UTs Scheme	Cash
91	Department of Agriculture and Biotechnology	Fruit Plantation scheme	State/UTs Scheme	In Kind
92	Department of Agriculture and Biotechnology	Jaivik Kheti Mission	State/UTs Scheme	Cash & In Kind
93	Department of Agriculture and Biotechnology	Kisan Samrudhi Yojana	State/UTs Scheme	Cash & In Kind
94	Department of Agriculture and Biotechnology	Krishi Yantra seva kendra	State/UTs Scheme	In Kind
95	Department of Agriculture and Biotechnology	Male pig distribution scheme	State/UTs Scheme	In Kind
96	Department of Agriculture and Biotechnology	Micro Irrigation tank	State/UTs Scheme	In Kind
97	Department of Agriculture and Biotechnology	Pashudhan Mitra Scheme	State/UTs Scheme	Cash
98	Department of Agriculture and Biotechnology	Pig trio distribution scheme	State/UTs Scheme	In Kind
99	Department of Agriculture and Biotechnology	Rajya Dairy Udhyamita Vikas Yojna	State/UTs Scheme	Cash

SNo.	Name of the implementing Ministry/Department	Scheme Name	Category	Benefit Type
100	Department of Agriculture and Biotechnology	Sakamvari Yojana	State/UTs Scheme	Cash
101	Department of Agriculture and Biotechnology	State Micro Irrigation scheme	State/UTs Scheme	In Kind
102	Department of Agriculture and Biotechnology	Sugercane Development Yojana	State/UTs Scheme	Cash & In Kind
103	Department of Agriculture and Biotechnology	Sukhshma Sichai yojana	State/UTs Scheme	In Kind
104	Department of Agriculture and Biotechnology	Transport subsidy	State/UTs Scheme	Cash
105	Department of Agriculture and Biotechnology	Ukti bij sambardhan Yojana	State/UTs Scheme	Cash & In Kind
106	Department of Culture	Artha Bhavgrastha Lekhako Kalakaro evam Unke Ashrito ko Vittya Sahayata	State/UTs Scheme	Cash
107	Department of Culture	Chhattisgarh Kalakar Kalyan Kosh se Arthik Sahayata Yojana	State/UTs Scheme	Cash
108	Department of Culture	Chinhari Yojana	State/UTs Scheme	Cash
109	Department of Fisheries	Jhinga sah Machhali Palan	State/UTs Scheme	Cash & In Kind
110	Department of Fisheries	Mausami Talabo me Span Samvardhan Hetu Sahayata	State/UTs Scheme	In Kind
111	Department of Fisheries	Shikshan Prashikshan	State/UTs Scheme	In Kind
112	Department of Food and Civil Supplies	DBT - Chana	State/UTs Scheme	In Kind
113	Department of Higher Education	BPL Scholarship- Higher Education	State/UTs Scheme	Cash
114	Department of Rural Industry	Design evam Takniki Vikas Karyashala	State/UTs Scheme	In Kind
115	Department of Rural Industry	Hastashilp me Karyasheel Punji Anudan - Shilpiyo se samagri kray	State/UTs Scheme	Cash
116	Department of Rural Industry	Hastashilp me rajya puruskar yojana	State/UTs Scheme	In Kind
117	Department of Rural Industry	Hastashilp Vikas Yojana - Job Work Sangrahan	State/UTs Scheme	In Kind
118	Department of Rural Industry	Hastashilpa ke liye Bima Yojana Anudan	State/UTs Scheme	In Kind
119	Department of Rural Industry	Hastashilpa Pratispardha evam Award Anudan	State/UTs Scheme	In Kind
120	Department of Rural Industry	Hastshilpo ko Prashikshan Anudan	State/UTs Scheme	In Kind
121	Department of Rural Industry	Mulberry Resham Vikas Evam Vistar Yojana	State/UTs Scheme	Cash & In Kind
122	Department of Rural Industry	Pradarshini Prachar evam Prasar	State/UTs Scheme	Cash

SNo.	Name of the implementing Ministry/Department	Scheme Name	Category	Benefit Type
123	Department of Rural Industry	Scheme for Development of Silk Industry - Tassar	State/UTs Scheme	Cash & In Kind
124	Department of Rural Industry	Shilpi hetu Design evam Vikas Shiksha	State/UTs Scheme	In Kind
125	Department of Rural Industry	Shilpiyo ko masik Aarthik Sahayata	State/UTs Scheme	Cash
126	Department of School Education	CT OBC POST MATRIC STATE SCHOLARSHIP FOR STUDENTS OF CLASS 11TH AND 12TH	State/UTs Scheme	Cash
127	Department of School Education	CT OBC PRE MATRIC STATE SCHOLARSHIP FOR STUDENTS OF CLASS 6TH TO 10TH	State/UTs Scheme	Cash
128	Department of School Education	CT SC KANYA SAKSHARTA PROTSAHAN STATE YOJNA FOR GIRLS OF CLASS 6TH	State/UTs Scheme	Cash
129	Department of School Education	CT SC POST MATRIC STATE SCHOLARSHIP FOR STUDENTS OF CLASS 11th and 12TH	State/UTs Scheme	Cash
130	Department of School Education	CT SC PRE MATRIC STATE SCHOLARSHIP FOR STUDENTS OF CLASS 3RD TO 10TH	State/UTs Scheme	Cash
131	Department of School Education	CT ST KANYA SAKSHARTA PROTSAHAN STATE YOJNA FOR GIRLS OF CLASS 6TH	State/UTs Scheme	Cash
132	Department of School Education	CT ST PRE MATRIC STATE SCHOLARSHIP FOR CLASS 3RD TO 10TH	State/UTs Scheme	Cash
133	Department of School Education	CT STATE SCHOLARSHIP FOR STUDENTS BELONGS TO FAMILY ENGAGED IN UNCLEAN OCCUPATION	State/UTs Scheme	Cash
134	Department of Social Welfare	Mukhyamantri Pension Yojna	State/UTs Scheme	Cash
135	Department of Sports	Khel academy- scholarships	State/UTs Scheme	Cash
136	Department of Sports	Khilario ko protsahan- Award money	State/UTs Scheme	Cash
137	Department of Sports	Khilario ko protsahan- scholarships	State/UTs Scheme	Cash
138	Department of Sports	Khilariyon Ko protsahan - Track suit distribution	State/UTs Scheme	In Kind
139	Department of Technical Education	BPL Scholarship - Technical Education	State/UTs Scheme	Cash
140	Department of Technical Education	BPL scholarship -ITI	State/UTs Scheme	Cash
141	Department of Technical Education	Craftsman training and apprenticeship training scheme	State/UTs Scheme	In Kind

SNo.	Name of the implementing Ministry/Department	Scheme Name	Category	Benefit Type
142	Department of Technical Education	Laptop distribution scheme	State/UTs Scheme	In Kind
143	Department of Technical Education	Laptop distribution scheme	State/UTs Scheme	In Kind
144	Department of Technical Education	Merit Scholarship	State/UTs Scheme	Cash
145	Department of Technical Education	Merit scholarship - ITI	State/UTs Scheme	Cash
146	Department of Technical Education	Yuva shamata vikas yojana	State/UTs Scheme	In Kind
147	Food Department	DBT Kind- Sugar	State/UTs Scheme	In Kind
148	Forest Department	Hariyali Prasar Yojana	State/UTs Scheme	In Kind
149	Forest Department	Mukhyamantri Bans Badi Yojana	State/UTs Scheme	In Kind
150	Forest Department	Tendu leaf bonus	State/UTs Scheme	Cash
151	Forest Department	Tendu Patta Yojana	State/UTs Scheme	Cash & In Kind
152	Labour Department	Antyeshti Yojana	State/UTs Scheme	Cash
153	Labour Department	Chhatra/Chhatra hetu Vishesh Coaching Yojana	State/UTs Scheme	In Kind
154	Labour Department	Durghatana Me Chikitsa Sahayata Yojana	State/UTs Scheme	Cash
155	Labour Department	Gambheer Bimari Hetu Chikitsa Sahayata Yojana	State/UTs Scheme	Cash
156	Labour Department	Medhavi Chhatra/Chhatra Shiksha Protsahan Yojana	State/UTs Scheme	Cash
157	Labour Department	Mukhyamantri Cycle Sahayata Yojana	State/UTs Scheme	In Kind
158	Labour Department	Mukhyamantri Nirman Majdoor Kaushal Vikas Parivaar Sashaktikaran Yojana	State/UTs Scheme	In Kind
159	Labour Department	Mukhyamantri Shramik Aujaar Sahayata Yojana	State/UTs Scheme	Cash
160	Labour Department	Mukhyamantri Silai Machine Sahayata Yojana	State/UTs Scheme	In Kind
161	Labour Department	Rajmata Vijayaraje Kanya Vivah	State/UTs Scheme	Cash
162	Labour Department	Suraksha Upkaran Yojana	State/UTs Scheme	Cash
163	Labour Department	Vishvakarma Durghatana Mrityu Par Anugraha Rashi Bhugtaan Yojana	State/UTs Scheme	Cash
164	Ministry of Women and Child Development	DBT - Salt	State/UTs Scheme	In Kind

SNo.	Name of the implementing Ministry/Department	Scheme Name	Category	Benefit Type
165	Social Welfare Department	Sukhad Sahara Scheme	State/UTs Scheme	Cash