NASSCOM®

NASSCOM's Feedback to the Ministry of Electronics and Information Technology on Strategy for National Open Digital Ecosystems (NODE)

31.05.2020

Feedback on the Consultation Whitepaper on Strategy for National Open Digital Ecosystems (NODE)

At the outset we would like to congratulate the Ministry of Electronics and Information Technology (MeitY) for taking this positive step towards enabling a strategy for an open ecosystem to leverage digital platforms for transformative social, economic and governance impact, through a citizen-centric approach and seeking public comments on the proposed framework. [i]

NODE is a powerful concept that can truly transform governance and citizen services. The consultation paper has rightly identified the key concerns in terms of the governance framework, the financing model and other risks like potential exclusion of certain users and builder groups, data security & privacy-related risks, weaponisation of the delivery platform or data.

Realising the potential of NODE will require appropriate incentives within the different departments of the Government to not only implement GovTech 3.0 but to implement it well. It will require identification of the right use cases which serve the greatest needs of the citizens. Finally, it will require a deep and broad participation of the industry and end users to ensure that the solutions are embraced and are value for money.

The Government should aim to develop the core blocks of the NODE and seek to develop an ecosystem where the industry is both able to develop and operate the services through business models which ensure that the NODE continues to develop and pay for itself. Many of the use cases discussed in the consultation paper can be considered as good examples for transformation into a NODE in a manner where the potential is fully developed.

Use of appropriate technology can be a key factor in unlocking the potential of a NODE. For example, as noted in Niti Aayog's recent paper on Blockchain, Governments should pay special attention to decentralised networks where peer-to-peer transactions can create more socio-economic value. Sectors of governmental intermediation where a state entity is involved just for ledger maintenance or collecting state dues but is not adding value to the transaction can be relooked to assess how government's role can be redefined in those sectors. The Government may explore Blockchain use in land-record and title management, payment systems, education certification management, immunisation supply chain management etc. Overall, we recommend use of open source software, open APIs and open standards.

There is a lot of effort involved in breaking down siloes and delivering joined-up services by the Government. Therefore, an implementation plan may consider agency design of entities like Nordic Institute for Interoperability Solutions (NIIS), Singapore's Government Technology Agency (GovTech), UK's Government Digital Service (GDS) to ensure an appropriate apparatus to facilitate development of NODEs. Different parts of the Government will need to align with each other. Government may also benefit from international cooperation. Memorandum of Understanding (MoU) with clear terms of co-operation may assist this.

Our Question wise feedback is provided below:

On the guiding principles for NODE

1. **Please comment on the guiding principles defined in Section 4 and indicate whether there are any principles you would add/ amend/ drop. Please provide reasons for the same.**

Response:

- Principle 2: Principle of reusability and shareability for the design of delivery platforms.

Recommendation:

Evolutionary Architecture as an additional principle is important and should be considered. Given that NODEs can evolve in ways that we may not be able to imagine at present, the architecture must evolve, and will have to be built as loosely coupled micro-services preferably interacting with Events and messages. Meta data should drive the discovery of these services with each other. This will allow the architecture to evolve instead of requiring the platform to be junked should it be unable to evolve with changing circumstances. A good example is plugin architecture.

- Principle 5: Delivery platforms under NODE should adopt an agile, data-driven development method.

Recommendation:

We agree that the system design should incorporate continuous integration and continuous development principles which will help services delivery systems adapt quickly to changing business requirements. Concepts such as DEVOPS and MLOPS should be implemented. The guidelines for open source and agile development should incorporate open source libraries. Examples of such open source libraries include GitHub, GitLab, Gitea, GNU Savannah, GitBucket and Gogs.

- Principle 14: Delivery platform should be analytics driven and generate insights to improve platform performance, robust policy-making and design of new solutions and services for users.

Recommendation:

The success of NODE will depend upon value creation for stakeholders. The government service delivery platforms should have high data crunching capabilities, i.e., it should have the ability to convert data into useful information.

Example- The Government of Rajasthan initiated the 'Big Data Environment Project' in 2018 to build a *"state level integrated data platform that will become a common source of structured & unstructured data for data mining and analytics initiatives for all government departments."*[ii] This is expected to enhance citizen services and engagement and increase efficiency in cross-functional operations between various government departments.

In addition to the principles defined in Section 4 of the NODE Consultation Paper, the following principles should be incorporated into the Guiding Principles for NODE:

1.1 Principles Related to the Architecture of the NODE

1.1.1) Need for Common Identity Framework- There is a need to enable users to use a single/common identity for accessing different government platforms under the NODE framework. This will make the process of accessing e-governance portals hassle-free for citizens, where they do not have to create multiple accounts for accessing multiple portals.

Example: A citizen 'X' creates an account on the income tax e-filing website. X should be able to use the same account (i.e. User ID and password) to login/register on e-Vahan to apply for a driving licence.

1.1.2) Ensure Quality of Service (QoS) related with Availability and Resilience of Systems: There is a need to ensure 'high availability' of system architecture by having a Business Continuity Plan and Disaster Recovery (BCP & DR) strategy in place.[iii] This will ensure availability of e-governance services without significant disruption, as well as prevent data loss in the event of a system failure. It should also implement concepts of auto-recovery for systems. In other words, there needs to be resilience in the compute capability (the process can restart at any time) as well as resilience in the state or data (no data loss, and the data remains consistent).

The UK recognised the importance of securing critical network and information systems that are critical for provision of digital and essential services, and in 2018 enacted the Security of Network and Information Systems Regulations (NIS Regulations) which implement the 2016 EU NIS Directive.[iv] For instance, Regulation 10(2) of the NIS Regulations stipulates that an 'operator of an essential service' must take "appropriate and proportionate measures" to prevent/minimise the adverse impact of incidents affecting the security of the network and information systems used to provide an essential service, with a view to ensuring the continuity of those services.[v]

The Quality of Service (QoS) parameters alongwith BCP & DR strategy must be defined at the concept level to ensure resilient systems. We outline some principles for the proposed BCP & DR strategy below:

a) **Regulatory and Department Leadership Support by MeitY**: If the senior management and leadership of a government department provide support to the business continuity (BC) and DR requirements due to clear directions and guidelines from MeitY, the remaining government staff is more likely to comply with the BCP&DR strategy, making it more effective overall.
b) **Risk Assessment**: This refers to a determination of scenarios which might disrupt the working of the information system alongwith assessing the impact of the disruption and the likelihood of its occurrence. One way of doing this is by giving a risk score to a particular disruption scenario alongwith assessing the government's appetite (i.e. tolerance for that risk); in cases where a high risk score is given to a particular disruption scenario, the government should formulate a response strategy to deal with that risk (should such a risk occur). Examples of responses are suspension of the disruptive activity or getting insured or providing backups.
c) **Business Impact Analysis (BIA)**: BIA is the most critical aspect of a BCP&DR strategy. BIA refers to the process of identifying a department's critical activities and resources, and assessing the severity on the government department, should there be any disruption to the activities or availability of the resources. The BIA helps in deciding how quickly a

particular activity should be resumed in the aftermath of an incident. BIA differs from risk assessment to the extent that BIA is not used to determine what the disruptive incident may be (which is a risk assessment output).[vi]

d) **Business Continuity Plans (BCP)**: The BCP is mainly developed on the basis of the risk assessment and BIA to ensure that the BCP accurately reflects the department's needs and specific circumstances. The objective behind the BCP is to stabilise the situation and ensure the continuity of a department's operations notwithstanding the occurrence of an incident.

e) **Adoption of International Standards:** We further recommend that to ensure QoS related to availability and resilience of information systems, the government consider adoption of international standards for management systems such as ISO 22301 or benchmark its parameters against such standards.[vii]

f) **Provision of Primary Data Centre (PDC) and Disaster Recovery Site/Data Centre (DRS)**: Based on BIA and BCP, government departments should provide for a PDC and DRS which should be located at an appropriate distance from each other based on several factors; these include possibility of occurrence of natural disasters and political unrest at the site of the PDC. Further, the DRS should have the same set of services as the PDC so that the former can act as a backup in case of failure of the PDC. The government departments must also ensure that the data centres have the necessary international certifications. [viii]

g) **Conduct drills regularly to determine the efficacy of BCP & DR strategy**: Government departments must conduct drills periodically by simulating challenging conditions to test the efficacy of their BCP & DR strategy. Common drills include table-top exercises, structured walk-throughs and simulations.

h) **Periodic reviews to improve the BCP**: This is crucial given the changes in technology. It is imperative that BCP reviews include lessons learnt from incidents which have occurred in the past.

i) **Cyber resilience to protect especially against cyber-attacks and data breaches**:

Cyber resilience is the ability to prepare for, respond to and recover from cyber-attacks.[ix]

Recently, Scotland published a Cyber Resilience Framework 2019-2020 aimed at providing *inter alia* clarity and assurance to individual organisations, Ministers, the Scottish Parliament and the public that appropriate levels of cyber resilience are in place across the Scottish public sector and its individual subsectors.[x] One of the four key domains of the Cyber Resilience Framework is to understand, assess and systematically manage risks to the network and information systems supporting essential services.[xi] It is important to note that the Scottish Cyber Resilience Framework aligns with key wider cyber-related requirements under the EU General Data Protection Framework (GDPR), the EU NIS Directive and other standards.

In the context of cloud, cyber resilience includes the following:

- Determining which data and services will be moved to the cloud
- Establishing a prioritised list of government services for cloud migration- these services refer to information systems where unavailability for any significant period of time would be unacceptable, e.g. land or tax records.
- Implementing pilot projects to test established technical and policy requirements for use of cloud computing in the public sector

- Updating public policy, as needed, to enable the use of cloud computing for cyber resilience
- Developing the technical process of migrating data and services to the cloud
- Relying on established best practices for proof of efficacy of security practices in place- Government departments could require appropriate proofs of the efficacy of security capabilities in products and services procured from vendors
- Conducting regular reviews of the policies and processes in place- To respond effectively to any cyber threat, government departments must conduct regular risk assessments and cybersecurity exercises. Additionally, the government could evaluate whether new technologies may be used in cyber resilience efforts; accordingly, policies and processes may need to be rewritten to enable the use of such technologies in cyber resilience.

1.1.3) Need for a Strong Cyber Security Framework: Cyber-security should be a foundational principle of such information systems with a robust cyber security framework being part of its design. At present, there is a lot of ambiguity regarding data access related aspects including Data Classification guidelines – how restricted/classified/unclassified information will be stored and accessed. The proposed cyber security framework will help address this.

1.2 Principle(s) Related to Change Management

The biggest challenge for any government service delivery platform would be change management. Change management is related to the concept of agility of the platform or the ability to adapt the platform to changing needs. There must be clear guidelines on change management.

1.3 Principle(s) Related to Procurement

The General Financial Rules on procurement are not conducive for opex-based buying. The procurement guidelines need to be amended to include cloud services and opex-based purchase mechanisms. This is because systems like NODEs require continuous improvement of technology and technological upgrades should not be stuck due to financial process blockers.

1.4 Principle(s) Related to Infrastructure

1.4.1) In order to make government services delivery platforms inclusive and a success, there is a need to improve broadband infrastructure in the country. The government should consider adopting alternate technology like satellite, TVWS, 5G etc. to make broadband ubiquitous.

1.4.2) Further, delivery platform solutions must be available in local languages, given the diversity of languages spoken in India.

1.4.3) To ensure inclusivity of citizens with varying socio-economic backgrounds, access to the entire infrastructure and apps should be built to work on low bandwidth and on low end devices.

2. For these principles (either individually or collectively), are there platforms (in India or globally) that you consider as benchmarks (from a best practice standpoint)?

Recommendation:

e-Estonia is a model worth emulating. Estonia currently ranks quite highly in the UN E-Government Development Index.[xii] Estonia's citizens are able to access a wide range of services online using secure digital IDs which include internet voting, making digital payments, and accessing full health records.[xiii] 99% of the public services are available online 24/7 and it is estimated that e-Estonia has saved the country "800 years of working time".[xiv] Estonia's e-Residency program under the e-Estonia model is particularly lauded for its simplicity and completely digital nature.[xv]

The X-Road data exchange system of e-Estonia is particularly remarkable. Under this system, the citizen's data is owned by the citizen and not the state. This means that any data exchange of a citizen's data can take place only with the consent of a citizen. E.g. a dentist will need to seek the citizen's permission before the former can share the data with another healthcare provider.[xvi]

NASSCOM shall be pleased to facilitate discussions with the Estonian Government to discuss best practices and implementation learnings.

On Delivery Platforms

3. **What are the biggest challenges that may be faced in migrating from a 'GovTech' 1.0 or 2.0 approach to a NODE approach (e.g. inter-departmental systems integration, legacy systems modernization, poor usability, and poor data quality)? How might these be overcome?**

Response:

NODE envisions an ecosystem-based approach to service delivery, where central and state governments achieve interoperability across departments by facilitating seamless flow of data. Presently, multiple touchpoints exist between the government and citizens in India, and ministries and departments operate in silos with regards to data collection and processing. Making service delivery unified through the creation of single touchpoint between the government and end-users is crucial. Moving to an ecosystem-based approach will also require a shift in the way the government engages with the broader community of various stakeholders (public and private actors who will create new solutions on top of the core delivery platform and end-users who will use the product) alongwith strong governance frameworks around data access and sharing.

Specifically, we foresee the following challenges in migrating from a 'GovTech' 1.0 or 2.0 approach to a NODE approach:

- Different government departments are at different stages of their IT evolution, ranging from those with very advanced technology to those not having sufficient PCs. Getting all to the same level on a common platform will be a challenge.
- Ministries do not easily share data with each other.
- The data shared between government departments may be in various formats and would require to be cleansed before using it on a common platform such as NODE. Further, datasets by different government departments could be contradictory which could make it difficult to determine which dataset is trustworthy.

- With respect to cloud adoption, there may be certain difficulties such as moving to a cloud design thought process, deploying on clouds same as you do on-premises and cloud knowledge and fear of new technology.
- Finally, migrating from a 'GovTech' 1.0 or 2.0 approach to a NODE approach requires actions beyond 'business as usual'.

Recommendations:

3.1) **Incentive:** The migration calls upon the government departments to adopt a mission mode and will require appropriate incentives. We do not have a specific recommendation on how this might be achieved. It may be in terms of a legislative mandate be directional like the Fiscal Responsibility and Budget Management (FRBM) Act, 2003 – we may of course learn from our experience of the FRBM Act. The migration will need an all-round support; while the IT departments in the Governments will have an important role, the migration will need to be driven by the office of the Prime Minister and the offices of the respective State Chief Ministers.

3.2) **Re-skilling:** Officials may not be well versed with technology, especially at the grassroots and local administration levels which may be a hindrance to adoption and engagement. This requires re-skilling or re-training of key officials in the use of technology.

3.3) **Focus on proactive awareness of the benefits**: One of the potential impacts of NODE could be digital infrastructure becoming the focal point for facilitating the delivery of services and solutions, instead of officials doing the job manually. The sense of redundancy as technology replaces government staff might be a limiting factor for adoption of the NODE approach at several levels. Therefore, the Government will need to proactively create awareness and ownership within the different parts of the government to ensure success of this initiative.

3.4) **Availability of finance**: There will be a need for an attractive financing framework so that the Government departments or States are not unduly deterred by costs. GovTech companies (i.e. companies which provide technological solutions to the government) often struggle with access to funding given the long sales cycles involved in doing business with the government. The traditional finance market often does not account for this, and therefore, provides limited financing options to GovTech companies. Philanthropic and private sector funding should be encouraged as alternative funding options.

3.5) **Dealing with Legacy Systems:** Legacy systems that delivery platforms depend upon are often barriers for the platform to scale. It is important that legacy systems should be modernised (if feasible) or junked.

4. In your opinion, should all delivery platforms be 'open source' or are 'open APIs' and 'open standards', sufficient? Please elaborate with examples.

Response:

Open source innovation fosters collaboration and open source has been used increasingly by governments for digital government transformations.[xvii] An example is the OpenCerts program in Singapore, an open source platform to verify educational credentials as well as provide a marketplace for online players to offer commercial applications to meet citizen needs.[xviii] Another example is Estonia's X-road which is built on an open source platform.

Recommendation:

We recommend that the platforms should be open sourced so that the community can collaborate and work to improve the platform. For the components or software used to 'build' the platform/NODE, we recommend that open source should be preferred, but not mandated; use of open source software (OSS) will help to prevent the problem of vendor lock-in. This is in line with MeitY's "Policy on Adoption of Open Source Software for Government of India".[xix] This Policy stipulates that all government organisations, while implementing e-Governance applications and systems must include a specific requirement in Request for Proposal for all suppliers to consider OSS alongwith Closed Source Software (CSS) while responding; suppliers are required to provide justification for exclusion of OSS in their response.

Further, some principles which can be used for choice of a delivery platform in any given case are:

4.1) The best IT system should be used which may be Commercial, Off-the-shelf (COTS) or Open Standards based. The focus should be mainly on service delivery by the IT system.

4.2) The standards and APIs should be Open Standards based which will ensure inter-operability. Open standards are also critical in ensuring that the different components of a large project can be built independently.[xx]

Open standards have been adopted in public procurement policies of other jurisdictions such as Japan. In June 2007, Japan's Ministry of Economy, Trade and Industry published the 'Interoperability Framework for Information Systems' aimed at ensuring interoperability by *"utilising open standards which many vendors can implement and adopt."*[xxi]

4.3) Data exchange and data sharing must be as open as possible.

4.4) The NODE strategy should be harmonised with the existing policies on open APIs and open standards formulated by the Indian government.[xxii]

4.5) The government should establish a web 3.0 based semantic ontology of all service and known data sources with documented ontology for 3rd party to value add and provide for next generation of artificial intelligence.

On governance

5. Do NODEs across sectors require common governance frameworks and regulatory/ advisory institutions to uphold these? Or is it sufficient for each node to have an individual governance construct? If a common framework is required, please elaborate the relevant themes/ topics e.g. financing, procurement, data sharing.

Recommendation:

Much of the governance model is similar across NODEs. There should definitely be a common governance framework which should form the basis for governance across NODEs. However, specific policies can be implemented keeping in mind a sectoral NODE's specific requirements, alongside the common governance framework.

We have commented on specific principles required with respect to procurement, financing, data sharing etc. in our response to questions 1 (on the guiding principles for NODEs), 6 and 7.

6. **Are you aware of any innovative financing models that could be deployed to build NODEs? If yes, please describe along with examples e.g. PPP models or community crowdfunding models.**

Recommendations:

6.1) The financing model is dependent on the specific sector and should take into account factors such as the nature of data collected, citizens' ability to pay and the extent to which private players are active within the sector. Multiple financing structures at various levels of the NODEs are also possible.

6.2) Government departments could play an active role in monetisation of the NODEs through indirect methods. Some examples are:

i. Use of NODE as a platform for G2B2C transactions which can monetise the entire platform and make it self-sustaining- Initially there was a plan for Aadhaar to charge Rs 1 per authentication. That could have paid for the project within a short period.
ii. A NODE for transport may be used for auto-insurance and auto-sales obviating the need for government funds to finance the NODE.

6.3) We believe that financial sustainability should be a key design consideration. That may require a Special Purpose Vehicle for each NODE and the onboarding of the best resources and the best technologies.

7. **What are some potential risks that open digital ecosystems can leave citizens vulnerable to, for example, risks related to data privacy, exclusion, having agency over the use of their data etc.? What types of overarching guidelines and/or regulatory frameworks are required to help mitigate them?**

Based on our consultations with members and other stake holders, we envisage four broad categories of potential risks. These are as follows:

I) Legal Risks

- Privacy concerns- Concerns regarding privacy and data security are of primary importance. It is important that the legal framework is finalised in terms of the Personal Data Protection Bill (PDPB)[xxiii]. Data will have to be shared within government agencies and with private players. In the absence of adequate checks and balances, NODEs risk misusing and compromising users' data.
- Heterogeneous licences across datasets- For the democratic use of data by re-users, it is necessary to ensure that access to data is granted across datasets. Access to data should not be selective and opaque. That will lead to incomplete openness of the data and create a trust deficit with the users and re-users of data.
- Difficulties with data ownership- Certain datasets may include data owned by multiple stakeholders with different data governance policies. Currently, while the focus is on public data, maximum value of Open Data will be derived when we combine public data, business data, and personal data.[xxiv] Most new services that will be created in the coming years will be based on a combination of these datasets. When all datasets are stacked, several organisations will be able to claim ownership of control over a dataset. It will be necessary to clarify, where needed, who is the ultimate owner of the data, in line with the PDPB and in case of non-personal data, in terms of the intellectual property rights (IPR) or trade secret or any other appropriate principles.

- Risks related to user skills- Given the disparity in education and skill levels in India, it can be expected that there will be two types of legal barriers for open-data platforms.
  i. Language barrier for users to give consent- Since most of the citizens in India speak in local dialects, it will be difficult for the users to properly understand the consequences of sharing their data for open data platforms if consent is not sought in their language of preference. This will be a challenging task for corporations and the government. For critical user data, it will be ideal for the users to sufficiently understand the consequences of data sharing and take their informed consent.
  ii. Skills related to information literacy and domain knowledge- Given the varied level of basic skills, it is possible that open data will not equally benefit all social categories. It may even lead to a deterioration of living conditions for a part of the population, while disproportionately benefitting a group that has the necessary skills to make use of the newly released information.[xxv] However, such risks are inherent to any innovation and only reflects the extent of the digital divide. To a large extent, such risks are beyond the scope of Open Data, and relate more to level of education and information literacy.
- Monetising of data: Monetising the platform and the data must be carefully monitored to prevent any exploitation. Monetisation of data that goes beyond the purpose for which data is collected or that threatens user's privacy or security of the system must be checked. Effective governance principles that address this threat should be put in place.

II) Governance Risks

- Inconsistent public policy- Lack of consistency in political behaviors can put the initiative at risk. Re-users of data will need to be confident that the Open Data Policy is sustainable so that datasets are updated and continuously made available. If Open Data Policy remains a project of a specific team, then the willingness to implement the project will be questioned as soon as another government comes to power. For a re-user to find a business model and implement a sustainable service, it is necessary that data sources are stable and maintained over time. Re-users can react strongly to any adverse signal from the authorities. However, if Open Data Policy is rooted in the administrative culture and operations, if it is supported by a cultural shift in public administrations, then it is possible to decrease the risks that the Open Data Policy will be overturned.[xxvi]
- Identifying the relevant administration level- A major challenge is, therefore, to find a balance in the intervention of different political levels, between state intervention (central or federal) that should ensure the consistency of the released datasets and local responsibilities. If each authority makes diverse choices regarding reuse conditions and formats given its context, they may cause a risk of fragmentation of the initiative at the expense of the potential reuse of data released beyond the local territory. Therefore, it is important that there is a balance in the intervention of different political levels between states interventions that ensure that there is consistency of the released datasets and local responsibilities.

III) Data quality Risks

- Data accuracy and bias- If the data used for the open data platform is solely generated by the government, data biases and inaccuracies may arise. Data may be influenced by political pressure and the context for which it is created may raise concerns regarding potential manipulation by the state.

- Interpretation and misuse of data- If the quality of data shared is of a poor quality and not representative of the bigger picture, decisions based on the data may be skewed and ineffective. There is also a risk that such decisions will lead to little attention for public value and addressing the societal problems but end up generating unfair revenue for the mala fide data re-user.

IV) Cybersecurity Risks

- Cybersecurity will be a constant threat to NODEs with state and non-state actors trying to exploit vulnerabilities. The threat will be more if it is a totally open system with two-way communication (unlike Aadhaar—where communication is essentially one way). So, the best of breed cyber security solutions needs to be deployed with strong accountability.To address some of these risks and ones highlighted above, we recommend that NODEs should adopt ISO27701 or equivalent and GDPR standards/ equivalent criteria as standards.

Recommendation(s) to address these concerns:

- Platform should be robust enough to collect security data across devices, users, applications servers and anywhere it resides through adoption of latest technologies like power of artificial intelligence to minimise cyber risk and data protection.
- Citizens should be able to control the access and propagation of the data by attribute. Citizens should also be able to see use of their data on the Government Platforms.
- Never let the sensitive data leave the platform, but rather the platform innovators come into the platform. This could be done in several ways (including Distributed Ledger Technology).
- The Government can extensively leverage Blockchain smart contract system to mitigate malicious actors manipulating information for various front end and backend access mechanisms. Our recommendation includes platform like Ethereum[xxvii], immutable storages like IPFS[xxviii].
- There is need for visibility/metrics and controls on every component to pinpoint issues efficiently, optimise and scale effectively, while having the assurance that security, compliance and polices are in place.
- A balanced approach comprising global cybersecurity and privacy standards alongwith a push towards indigenous solution requirements, is required.
- A trust-based environment is essential for mass adoption of innovative use cases.
- There is a need to prioritise security of cyber-physical systems, especially in sectors related to National Critical Information Infrastructure.

On Community

8. **What are effective means to mobilize the wider community and build a vibrant network of co-creators who can develop innovative solutions on top of open platforms? What can we learn from other platforms or sectors?**

Community participation is directly proportional to the value they see in co-creation. Value can be monetary or in other means. We believe a "Product Thinking" approach is important when conceptualising platform APIs and giving scope for the innovators to build on. Mobile communication of the future particularly the new 5G is going to play a critical role in the future world.

Government needs collaboration services that span messaging, conferencing, and telephony, social and collaboration, content management, data analytics and visualisation. There is also a need for tools that better connect their employees and information across boundaries, enabling remote and online collaboration and allowing citizens greater access to services and interaction with officials.

In the recent past, there have been some initiatives undertaken by the Government in this regard.

For instance, the Aadhaar ecosystem was envisaged with an aim to foster innovation. Similarly, the Open Data project[xxix] was also supposed to spawn big innovation. However, these initiatives have not been able to realise their full potential till now. Thus, it becomes necessary to analyse why innovation has not taken off, is it funding, it is mentorship, is it lack of technical skills, is it lack of capability to market products etc.? For the effective utilisation of the layered model of applications and products capitalising on top of delivery platforms, it is essential to have a vibrant community that innovates and supports the continued development and maintenance of such platforms. This assumes even more significance as open source software is increasingly adopted.

Recommendation(s):

- Platform should go beyond data and allow the participants to contribute back to the platform.

Example-Facebook gets data back from the partner network, which it effectively uses further to improve the value for partners thereby making the platform more valuable over time.

- The Government should allow private individuals, small communities and remote villages to invest in 5G antennae & edge compute and provide secured local connectivity for various services. A revenue sharing model can be established. CBRS spectrum model in many countries is an emerging model.[xxx]
- The Government should leverage emerging standard to leverage the DRM radio for dispersing data. It can even be leveraged for disaster management.[xxxi]
- Collaborative development models can be reviewed and adopted; an example is GitHub.[xxxii] Once there is data available and APIs available, the startup ecosystem will automatically get attracted. Initially this movement can be encouraged through means of hackathons etc. Later the system will get into a virtuous cycle.
- An effective and time-tested method in creating such vibrant communities is that of creating funded competing models to promote the culture and incentivise the process.

Example(s)-In the United States, City Innovate[xxxiii] published more than 50 challenges from state and local governments across the country. In response, tech companies now can propose solutions to these challenges, which governments can further implement.[xxxiv]

Similarly, in the United Kingdom, "GovTech Catalyst" uses a £20 million fund to pay suppliers to solve public sector problems using innovative digital technology. The public sector proposes complex problems (or 'challenges') that up to five suppliers are funded to work on for three months. If results are promising, up to two of those suppliers get to work on it for a year.[xxxv]

9. **Are you aware of any end-user adoption and engagement models that platforms have successfully adopted e.g. feedback loops, crowdsourcing use cases, offline awareness and on-boarding campaigns?**

Yes. Based on inputs of the members, we have been able to identify several end-user adoption and engagement models that have been successfully adopted and we have also made specific recommendations in this regard.

Example(s)- MyGov platform is a citizen-centric platform which empowers people to connect with the Government & contribute towards good governance.[xxxvi] It is aimed at creating a common platform for Indian citizens to crowdsource governance ideas from citizens.

An open-source model is another example. It refers to a decentralised software development model based on principles of open collaboration.[xxxvii] Peer production is the main principle of open-source software development; it consists of elements like source code, blueprints, and documentation for the public's disposal. Also, the computer code that underlies each main cryptocurrency and opens a blockchain project is the result of open-source software development.[xxxviii]

Recommendation(s):

- The Government should establish a crowdsourcing platform for executing lot of government work through a gig model. Platforms like Gigwalk is a good example of implementation in the private space.[xxxix]
- Community growth model from GitHub should be reviewed and adopted accordingly.

10. **Are you aware of any innovative grievance redressal mechanisms/models that go beyond customer support helplines to augment accountability to citizens? If yes, please describe along with examples.**

Yes. Based on inputs of the members, we have been able to identify several end-user adoption and engagement models that have successfully adopted, and we have also made specific recommendations in this regard.

Example(s)- In Brazil, through a social participation platform, 'Participa.br', the government has promoted an initiative engaging in the development of free software and in body communication tools, discussion forums, chat rooms, videos, maps, participation trails and other means of online social consultation. Since its creation, Participa.br has been hosting over 200 participatory processes and more than 30 public government consultations.[xl]

Similarly, the Japanese government has created a 'Digital Governance Idea Box 2017' as a venue to start discussions around e-governance issues and create a feedback loop.[xli]

In Finland, there has been an emphasis on openness and democratic principles in the digital era. Some examples of this development work include the Government's Project Register (HARE), established in 1999; and the otakantaa.fi website, established in 2000 to promote public discussion on government proposals; Hear Citizens project (2000-2005);

Government's Policy Program on Citizen Participation (2003-2007) and the on-going Democracy Network established in 2007.[xlii]

In Sydney, Australia, the Sydney's Community Consultation plan[xliii] offers a range of opportunities for residents, workers, community groups, business, government, and industry stakeholders to share ideas, insights, and feedback on the city projects and policies to help inform council decisions. The city government organises workshops and community meetings and roundtables, drop-in sessions, surveys, etc. which are analysed and fed into the decision-making process.

Recommendation(s):

- The above models present interesting insights into starting a participatory process which can help kickstart a community engagement process and present a route to augment accountability and promote a healthy sense of communal belonging.
- The principles followed by the City of Sydney to guide the government's approach in engaging the community in decision-making can also be considered.[xliv] These principles are as follows-

Integrity: engagement should be clear in scope and purpose.

Inclusiveness: engagement should be accessible and capture a full range of values and perspectives.

Dialogue: engagement should promote dialogue and open genuine discussion.

Influence: The community should be able to see and understand the impact of their involvement in consultations that the city conducts.

On designing and implementing NODES in your sector

11. Imagine designing a NODE in the context of the state or sector that you work in (please refer to Figure 4 and the Figures in Section 5), and describe -

11.1 The key challenge/ problem your NODE is seeking to address? What benefits will it offer?

Based on our consultations with members and other stake holders, we submit the following as recommendation from our end.

Recommendation(s):

- The NODE should be purpose-built infrastructures which can be customised based on any specific needs regardless of whether it is getting managed in the network, on the cloud or in the hybrid infrastructures.

11.2 The key building blocks for this node or key components of the delivery platform? Please list any challenges / barriers you may face in building this platform e.g., poor data quality, data is in silos, lack of common open standards and APIs, transition from legacy systems, etc. and how you may overcome these

Based on our consultations with members and other stake holders, the challenges/ barriers which might be faced when one is building this platform have been summarised as follows-

Challenges/Barriers

- Gov 2.0 or similar existing platforms which already exist carry ample of data in unstructured, silo database – How to bring the data, functionalities and legacy inputs to the new platform will be a challenge.
- Interoperability for APIs, multiplatform technologies along with legacy hardware / open platform will need scalable robust platform.

Recommendation(s) to overcome the challenges:

- Introducing Foundational Platforms for Employment, SMEs, Governance etc.
- Enabling Cloud Strategy, which is strong on governance, secure, multi-platform and strong on interoperability should be reviewed while making choices.

11.3 With reference to the 5 design principles on "Governance", please indicate what the governance model could look like for your NODE. What are some challenges/ barriers you may face in establishing a successful model e.g. inter-departmental coordination and strategies to overcome these?

No comments

11.4 The "Community" for your NODE – key stakeholders, how would they engage with the platform and build on top of it? What benefits would having a vibrant community offer and what additional use cases can be unlocked? Please list any challenges (e.g. incentivizing adoption, value sharing) and how you may overcome these?

No comments

On Support Required

12. **Are there any useful resources that you have come across that would help the broader community, as we build out this NODE approach?**

    The group executing NODE should consult the teams who implemented major Mission Mode Projects like Aadhaar, Income tax, MCA 21, GSTN etc. to get an idea of the challenges faced and how these can be overcome in a NODE setting.

13. **What kind of tools (e.g., case studies, workshops, online knowledge banks, access to experts, etc.) would be most useful for your organization/ department to enable you to take this approach forward?**

    Same as above. There are no readymade resources available for this.

14. **How would you like to engage further (e.g. individual consultations, workshops, etc.) as we build the strategy for NODE**?

We would appreciate the opportunity to engage with MeitY on NODE consultations through individual interactions and participation in workshops, and engagement with developers, public departments, and end-users.

Recommendation(s):

- A more structured and well laid out consultation process would be immensely helpful for the development of NODE framework. Some of our members have suggested that the consultation process followed by the Telecom Regulatory Authority of India (TRAI) is a good reference.[xlv]

TRAI follows a standard consultation process for every issue that it investigates:

– An expert committee in partnership with TRAI formulates a consultation paper, which is put in the public domain for comments and counter comments.
– The inputs on the consultation paper are published online by TRAI for visibility and transparency.
– There is an open house where industry experts, civil society members, and other stakeholders voice their views.
– TRAI's members also participate in consultations organised by civil society and industry associations.
– These inputs are collated together in the form of recommendations (can also be opened for a consultation) which is submitted to Department of Telecommunication (DoT) for consideration.

This process is often followed by several other departments including MeitY. We believe such a consultation process would make the development of the NODEs more inclusive, open, and transparent, thus espousing the key principles that MeitY envisages all NODEs to emulate.

---

[i] MeitY inviting public comments on Consultation Whitepaper on Strategy for National Open Digital Ecosystems- https://www.mygov.in/group-issue/inviting-suggestions-strategy-national-open-digital-ecosystems-node/
[ii] Abhishek Raval, 'Government of Rajasthan selects Teradata big data and analytics solutions', *Express Computer,* 25 July 2018; available at: https://www.expresscomputer.in/news/government-of-rajasthan-selects-teradata-big-data-and-analytics-solutions/23092/
[iii] 'High Availability' refers to elimination of single points of failure (SPOFs) by introducing redundancy which may be hardware or software based. On the other hand, disaster recovery is the process of getting a system back to an operational state when a system is rendered inoperative. Disaster recovery picks up where high availablity fails.
[iv] A copy of the NIS Regulations is available at: http://www.legislation.gov.uk/uksi/2018/506/made/data.pdf
[v] An 'operator of an essential service (OES)' is defined in Regulation 1(2) as 'a person who is deemed to be designated as an operator of an essential service under regulation 8(1) or is designated as an operator of an essential service under regulation 8(3)'.
[vi] Developing a BIA generally includes the following:
• Identify scope

• Identify key functional areas

• Identify critical functions

• Identify dependencies between departments and functions

• Determine RTO and RPO for each critical function

• Create BCP

[vii] ISO 22301 is a certification for business continuity management systems developed by International Organization for Standardization; for more information, see: https://www.iso.org/standard/75106.html
[viii] These are:
a. ISO 22301 Premium standard for business continuity

b. ISO 27002 (17799) - Deals with Information Security, if department is using Co-located data center or ISO/IEC 27017:2015 certification, an international standard that aligns with and complements the ISO/IEC 27002:2013 with an emphasis on cloud-specific threats and risks when using a Cloud Service provider.

c. ISO 9001, Quality Management - Record Retention and Data Availability

d. ISO 14001, Environmental Mgt - Emergency Preparedness and Response

e. TIA-942 standard based Tier 3 Data Center
[ix] This definition is taken from IT Governance; available at: https://www.itgovernance.co.uk/blog/the-it-governance-cyber-resilience-framework-how-it-works
[x] For more information, see: https://www.gov.scot/publications/cyber-resilience-framework/. The Scottish Cyber Resilience Framework is based on the Public Sector Action Plan on Cyber Resilience 2017/18.
[xi] For more information, see: https://www.gov.scot/publications/cyber-resilience-strategy-scotland-public-sector-action-plan-2017-18/pages/6/
[xii] See United Nations E-Government Survey 2018, p.86; available at: https://www.unescap.org/sites/default/files/E-Government%20Survey%202018_FINAL.pdf
[xiii] Nick Health, 'How Estonia became an e-government powerhouse', *TechRepublic*, 19 February 2019; available at: https://www.techrepublic.com/article/how-estonia-became-an-e-government-powerhouse/
[xiv] *Ibid*. Also, 'How do Estonians save annually 820 years of work without much effort?', available at: https://e-estonia.com/how-save-annually-820-years-of-work/
[xv] See 'What is Estonian e-Residency and how to take advantage of it?', *Xolo*; available at: https://www.xolo.io/articles/e-residency
[xvi] See, Mike Barlow and Cornelia Lévy-Bencheton, 'The smart nation where everyone owns their personal data', *Smart Cities World*, 24 October 2018; available at: https://www.smartcitiesworld.net/special-reports/special-reports/the-smart-nation-where-everyone-owns-their-personal-data
[xvii] Goh et al., 'The rise of open source to spur agile digital government', *World Bank Blogs*, 26 February 2020; available at: https://blogs.worldbank.org/governance/rise-open-source-spur-agile-digital-government
[xviii] *Ibid*
[xix] Available at: https://meity.gov.in/writereaddata/files/policy_on_adoption_of_oss.pdf
[xx] Elets News Network, 'Open Standards based e-Governance', *EGOV*, 1 October 2006; available at: https://egov.eletsonline.com/2006/10/open-standards-based-e-governance/
[xxi] Please refer to section 1.1 (Background and Objectives) of Japan's 'Interoperability Framework for Information Systems', available at: https://www.ipa.go.jp/files/000024895.pdf
[xxii] 'Policy on Open Application Programming Interfaces (APIs) for Government of India' is available at: https://meity.gov.in/sites/upload_files/dit/files/Open_APIs_19May2015.pdf; 'Policy on Open Standards for e-Governance' is available at: http://egovstandards.gov.in/sites/default/files/Policy%20on%20Open%20Standards%20for%20e-Governance.pdf
[xxiii] The Personal Data Protection Bill, 2019 was introduced in Lok Sabha by the Minister of Electronics and Information Technology. Available at: http://164.100.47.4/BillsTexts/LSBillTexts/Asintroduced/373_2019_LS_Eng.pdf
[xxiv] Martin, Sébastien & Foulonneau, Muriel & Turki, Slim & Ihadjadene, M. (2013). Risk Analysis to Overcome Barriers to Open Data. Electronic Journal of e-Government. Accessed at : https://www.researchgate.net/publication/289841742_Risk_Analysis_to_Overcome_Barriers_to_Open_Data
[xxv] Soloman Benjamin et al., 'Bhoomi: 'E-Governance', Or, An Anti-Politics Machine Necessary to Globalize Bangalore', Casum-m Working Paper, January 2007; available at: https://casumm.files.wordpress.com/2008/09/bhoomi-e-governance.pdf
[xxvi] Davies, T. (2010) "Open Data, democracy and public sector reform". Available at: http://www.opendataimpacts.net/report/wp-content/uploads/2010/08/How-is-opengovernment-data-being-used-in-practice.pdf
[xxvii] For more information, see: https://en.wikipedia.org/wiki/Ethereum
[xxviii] For more information, see: https://en.wikipedia.org/wiki/InterPlanetary_File_System
[xxix] Open Government Data (OGD) Platform India Report by National Informatics Centre. Available at: https://meity.gov.in/writereaddata/files/OGD_Overview%20v_2.pdf
[xxx] For more information, see: https://en.wikipedia.org/wiki/Citizens_Broadband_Radio_Service
[xxxi] For more information, see: https://en.wikipedia.org/wiki/Digital_Radio_Mondiale
[xxxii] For more information, see: https://help.github.com/enterprise/2.7/user/articles/types-of-collaborative-development-models
[xxxiii] For more information, see: https://www.cityinnovate.com/

[xxxiv] Refer to the article "Here Are All of the Current Startup in Residence Challenges" published at Government Technology, dated October 16, 2019. See: https://www.govtech.com/civic/Here-Are-All-of-the-Current-Startup-in-Residence-Challenges.html
[xxxv] https://www.gov.uk/government/collections/govtech-catalyst-information
[xxxvi]For more information, see: https://www.mygov.in/
[xxxvii] For more information, see: https://en.wikipedia.org/wiki/Open-source_model
[xxxviii] Refer to the article "What Is an Open-Source Model?" published on Medium.com, dated April 05, 2019. See: https://medium.com/@monetha/what-is-an-open-source-model-c4cb8eae2079
[xxxix] For more information, see: http://www.gigwalk.com/gigwalkers/
[xl] Box 5.5, "E-participation activities in Brazil", Gearing E-Government to support transformation towards sustainable and resilient societies, United Nations E-government survey 2018. Page 120; also see: http://www.participa.br
[xli] https://www.slideshare.net/hiramoto/170119-digital-government-in-japan
[xlii] Box 5.4, "E-participation activities in Finland", Gearing E-Government to support transformation towards sustainable and resilient societies, United Nations E-government survey 2018. Page 120.
[xliii] For more information, see: https://www.cityofsydney.nsw.gov.au/community/participation/community-consultation
[xliv] For more information, see: https://www.cityofsydney.nsw.gov.au/community/participation/community-consultation
[xlv] Refer to the open consultation process followed by TRAI at https://trai.gov.in/open-consultation