Response to the Consultation Paper on National Open Digital Ecosystems (NODE)

March 31,2020

By **Aman Nair, Elonnai Hickok &Arindrajit Basu**
With Inputs from **Gurshabad Grover**

About the Centre for Internet&Society 2

Executive Summary 2

General Comments 3

Question Response 7

The CIS Guide on NODEs 19

Part 1 : Framework For Assessing Viability Of New Nodes 21

Part 2: Broad framework of ‘Governance’ for proposed NODEs 26

Part 3: Framework For Analysing Existing Nodes 28

About the Centre for Internet&Society

The Centre for Internet and Society (CIS) is a non-profit organisation that undertakes interdisciplinary research on internet and digital technologies from policy and academic perspectives. The areas of focus include digital accessibility for persons with disabilities, access to knowledge, intellectual property rights, openness (including open data, free and open source software, open standards, open access, open educational resources, and open video), internet governance, telecommunication reform, digital privacy, and cyber-security. The academic research at CIS seeks to understand the reconfiguration of social processes and structures through the internet and digital media technologies, and vice versa.

CIS thanks Meity for the opportunity to provide comments on the National Open Digital Ecosystem.

Executive Summary

This Submission consists of the following parts:

1. General comments
2. Responses to the questions posed by the White Paper
3. A proposal for the implementation of a NODE framework.

Broadly speaking, we would recommend that before implementation NODE project in its present form should be **reassessed** for :

- Impact assessment on national security.
- Security standards and practices.
- Clarity on architecture of the NODE
- Lack of clarity on the implementation of the NODE
- Absence of clear evaluation metrics,
- Comparative and reliable appraisal of past efforts including Aadhaar and India Stack,
- Clear and uniform policy prescription delineating personal data from non-personal data and a governance framework for both
- Use of open source technologies beyond just open standards and open API's,
- Lack of clear institutional mechanisms for redress
- Drawing of clear 'red lines' on the scope of a NODE
- Adherence to public ownership, interest and benefit of the ecosystem
- Clearly articulated governance framework that explicitly constitutional rights and values
- When conceptualizing, designing, implementing and evaluating a NODE, the following questions are scrutinised for the entire ecosystem:
  Is there a law allowing for the creation of the NODE?
  Will the NODE enable an intrusion into fundamental rights? If yes,

- ○ Is an intrusion into fundamental constitutional rights necessary, i.e. is it the least intrusive option available?
- ○ Is the intrusion proportionate to the objective (e.g. public service delivery) being sought to be objective? Is the objective legitimate?

This re-assessment should serve as an essential pre-requisite before the NODE approach is rolled out.

General Comments

Below we outline our general comments to the white paper on National Open Digital Ecosystems.

1. **Need for a more nuanced articulation of objectives and scope**
   The white paper envisions the NODE acting as open and secure digital delivery platforms which enable innovation and transform service delivery. To ensure that the objectives of NODE can be met, we would recommend:

   Viability and Appropriateness of NODE: The underlying assumption present throughout the white paper is that the creation of NODEs would inherently improve the overall functioning of governance within a sector and have exponential positive benefits for citizens who are required to interact with the government. In this way the white paper assumes that all aspects of service delivery can be fully shifted to digital platforms and that a NODE will always be the correct solution. ***We recommend that the white paper consider an approach that assesses the viability of a NODE within a sector and what form a proposed NODE must take. A possible framework has been included as an annex to this submission.***

   Scope of NODE: A narrow definition of scope is critical in protecting against harms like function creep and surveillance. It is presently unclear if there are limitations on the scope of NODE with respect to what can be included in a NODE, who can access and use a NODE, and for what purposes. ***We recommend that the scope of the NODE is clearly articulated and reflects the findings from an assessment of viability.***

   Need for harmonization and integration into existing frameworks: Though the white paper references a number of existing frameworks including NDHB, NUIS, DIKSHA, and IndEA it is unclear if and how NODE will integrate or build off of these existing initiatives when implemented. For example, certain sections of the IndEA framework allude to the need for a strategy similar to the GovTech 3 strategy, and the need for greater inter ministerial collaboration as outlined in the white paper[1]. However these instances do not make mention of a singular government strategy divided into tiers in the same form as

[1] IndEA framework 1.0: "The need for adopting a holistic approach in the domain of e-Governance has become evident from the interoperability issues within and across multiple clusters of stand-alone applications developed by the States and Central Ministries over the last decade." http://egovstandards.gov.in/sites/default/files/IndEA%20Framework%201.0.pdf

the GovTech strategy outlined in the white paper. Furthermore, while the conception of NODEs in the white paper seems to be based primarily on the integration reference model, as well as the application and data reference models, outlined in the IndEA framework - there is no reference to this framework in the white paper. ***We recommend that the white paper clearly identifies where and how the NODE approach falls within the IndEA framework and other existing initiatives.***

2. Need for alignment with constitutional principles

India has a rich ethos of constitutional principles that guide and govern public service delivery projects. In this way, the Indian Constitution not only protects fundamental civil liberties but also views the state as playing a 'transformative' role in the mitigation of structural inequality and empowering vulnerable communities.[2] The NODE consultation paper does not refer to these principles and misses an opportunity for clearly grounding the governance framework in the legal context it is being implemented in. The key fundamental rights-right to equality, right to freedom of speech and expression, and the right to life (that includes both procedural and substantive rights to due process) must be considered as key tools of governance. Further, as evolved in the groundbreaking *Puttaswamy* judgement, the Right to Privacy is one that can be derived from any or all of these fundamental rights.[3] The protection of civil liberties can never be absolute but must always be balanced with other considerations-including the transformative role of The Constitution discussed above, and reasonable restrictions such as public order or national sovereignty.

We recommend that when conceptualizing, designing, implementing and evaluating a NODE, the following questions are scrutinised for the entire ecosystem:

- ***Is there a law allowing for the creation of the NODE?***
- ***Will the NODE enable an intrusion into fundamental rights? If yes,***
    - ***Is an intrusion into fundamental constitutional rights necessary, i.e. is it the least intrusive option available?***
    - ***Is the intrusion proportionate to the objective (e.g. public service delivery) being sought to be objective? Is the objective legitimate?***

3. Need for alignment with existing structures and institutions of governance

As per Article 12 of the Constitution, the state is responsible for guaranteeing fundamental rights whenever it undertakes a 'public function.' While the White Paper fails to clarify whether a NODE can be or will be entirely privately run, the institutions of governance that already exist in India must be responsible for ensuring the protection of fundamental rights. Therefore, while the 'single point of accountability' that the paper

[2] Gautam Bhatia, *The Transformative Constitution: A Radical Biography in Nine Acts* (Harper Collins,2019)

[3] Amber Sinha, " The Fundamental Right to Privacy: An analysis"https://cis-india.org/internet-governance/blog/the-fundamental-right-to-privacy-an-analysis (September 22nd, 2017)

espouses may be useful for designing and implementing the NODE, a single organization cannot effectively guarantee fundamental rights. A Special Purpose Vehicle (SPV) such as the example given in the White Paper might help set standards, implement the NODE and create rules of engagement, but it cannot replace the existing judicial and administrative mechanisms that guarantee redress. ***We recommend that efforts must be made to ensure that a NODE does not stifle access to courts and tribunals but instead works with these institutions to facilitate appropriate avenues of redress.***

4. **Need for harmonisation with existing policies and for critical governance frameworks for personal and non-personal data to be defined**

India's open digital ecosystem cannot be set up in a governance or policy vacuum. The White Paper fails to refer to any of the existing policy instruments that are looking to govern data in India-which causes an increase in regulatory uncertainty.

As of now, there exists a number of legal and policy endeavours engaging with the conceptualisation of data and a classification between personal and non-personal data in India.[4] The first is "community data", which is both in the Srikrishna Report that accompanied the draft Data Protection Bill in 2018 and the draft e-commerce policy. But there is no clarity on how the concept is used in the two documents. The Srikrishna Report proposes a collective protection of privacy by protecting an identifiable community that has contributed to community data. This requires the fulfilment of three key conditions: *1)* the data belong to an identifiable community; *2)* Individuals in the community consent to being a part of it, and 3) the community as a whole consents to its data being treated as community data. On the other hand, the Department of Promotion of Industry and Internal Trade's (DPIIT) draft e-commerce policy treats community data as "societal commons" or a "national resource" that gives the community the right to access it but government has ultimate and overriding control of the data, bringing it at odds with the consent framework in the SriKrishna report. Chapter 4 of the Economic Survey espouses data as a 'public good'-which includes non-personal data and any personal data held by the government as long as it is in anonymised form. Further, it allows for the data to be sold to private foreign firms without clarifying whether this includes foreign or domestic firms. Section 91 of the draft Personal Data Protection Bill also equates 'non-personal data' with anonymised personal data and enables the government to obtain access to these from several data fiduciaries.The NITI AAYOG also suggested the creation of 'data marketplaces' to enable analytics by various actors.

As many of these policies are still taking shape, we recommend that the NODE White Paper be finalised once there is clarity on the following questions and instruments:

1. ***Clear classification of personal and non-personal data***
2. ***Data producers' rights over data-including ownership and monetization***
3. ***A Personal Data Protection Bill is passed giving the data principal rights over their data and guaranteeing their privacy.***

[4] Arindrajit Basu, " We need a better AI vision", https://fountainink.in/essay/we-need-a-better-ai-vision-

4. ***Conceptualisation of non-personal data and how this conceptualisation fits into the NODE framework.***

Further we recommend that this document is developed in sync with the various policies that already exist and with the policies that are emerging - particularly those around data. MEITY had previously announced the setting up of a Committee that would answer critical questions around the governance of non-personal data. It is imperative that the report is published before the White Paper is finalised.

5. **Need for clarity in implementation of NODE**

   Though the white paper provides an overarching vision for the NODE, we recommend clarifying the following aspects with respect to how a NODE will be implemented including:

   a. **Technical clarity:** The architectural aspects of the NODE are unclear.
   b. **IP and ownership**: After a solution is developed using the NODE, it is unclear who will own the solution and any benefits that might come from the solution.
   c. **Access**: It is unclear the standards by which access to different parts of the NODE will be determined and by whom and via what process.
   d. **Permitted Use**: The permitted uses of the NODE by different stakeholders are unclear as are enforcement mechanisms for the same.
   e. **Terms of operation between public and private sector:** The relationship between the public and private sector is unclear as are the terms they will be operating under.
   f. **Standardization and standards:** The level of standardization across the NODE is unclear. For example, to what extent will different aspects of the NODE be standardized across departments. What standards will be adopted and who will make this decision?

6. **Need for engagement with terms and definitions**

   There are a number of places in the white paper where terms and concepts have been used without fully engaging with what they mean or recognizing challenges and lessons learned from the implementation of other digital governance projects in India. For example, the conceptualization of the delivery platform: pg.7 assumes data registries and exchanges can become a 'single source' of truth without recognizing the fluidity of data and the difficulty in ensuring baseline data is accurate. The aggregating ability of data registries leads to the cultivation of what Louis Amoore calls a 'data derivative'-a shared conglomeration of data that shapes individual futures without consulting the individual.[5] We recommend that the white paper include an assessment of the challenges that have been faced in previous initiatives in India.

[5] Louise Amoore, ' Data Derivatives:On the Emergence of a Security Risk Calculus for Our Time," (2011) 28 (6) Theory, Culture and Society 24,27

Question Response

1. **Question 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.

I. Design principles (1-5)[6]

A. Principle 1 (Page 14)

Be open and interoperable: Use and/ or build open standards, licenses, databases, APIs, etc. and promote interoperability. It helps realize inter-platform efficiencies, promotes competitive behaviour and guards against potential monopolies of unfair value capture. [7]

The white paper leaves a critical design aspect of NODEs undefined: rather than clearly describing the principles of "openness" that will be adhered to by the NODEs, the white paper notes that each NODE will 'have its own configuration of degree of "openness."' [8]Thus, the white paper fails to explicitly make NODEs recognise and comply with governmental policy on open source software, standards and APIs.[9] We recommend that NODEs wholly comply with the principles on open software that have been highlighted in:

* The National Policy on Information Technology, 2012;[10]
* Policy on Adoption of Open Source Software for Government, 2014[11] and
* Framework for Adoption of Open Source Software in e-Governance Systems, 2015.[12]

[6] Section 4.1, Pages 14-16
Ministry of Electronics and Information Technology Government of India, "Strategy for National Open Digital Ecosystem (NODE): Consultation White Paper," n.d., https://static.mygov.in/rest/s3fs-public/mygov_158219311451553221.pdf

[7] We thank our colleague Gurshabad Grover for providing his insights on , and writing out this paragraph
[8] https://static.mygov.in/rest/s3fs-public/mygov_158219311451553221.pdf, pg. 8
[9] For an indicative list, see https://cis-india.org/openness/files/economic-social-and-cultural-rights-in-india-foss/,
[10] https://meity.gov.in/writereaddata/files/National_20IT_20Policyt%20_20.pdf
[11] https://meity.gov.in/writereaddata/files/policy_on_adoption_of_oss.pdf
[12] http://egovstandards.gov.in/sites/default/files/Framework%20for%20Adoption%20of%20Open%20Source%20Software%20in%20e-Governance%20Systems.pdf

The Policy on Adoption of Open Source Software for Government is the most specific in this regard, and requires departments to make endeavours to ensure that all e-governance systems that are adopted by various Government organisations to run on open source software. The characteristics of "open source software", as used in the policy, are clearly defined: the source code shall be available free of cost for studying, modification and redistribution. [13]

Similarly, the vagueness around the principles of 'openness' should be changed to encourage compliance with the Policy on Open Application Programming Interfaces (APIs) for Government of India[14] when it comes to open APIs, and with the Policy on Open Standards for e-Governance[15] when it comes to open standards.

As an extension, NODEs should encourage that any associated initiatives and stacks (as examples, the white paper mentions the Modular Open Source Identity Platform, India Stack, Health Stack, NUIS)[16] should also meet the requirements of these policies.

We recognise that a level of flexibility may be permissible considering specific use cases. The exceptions in the aforementioned policies can therefore be suitably relied on as and when the case arises. For instance, the 2014 Policy on Adoption of Open Source Software forGovernment allows for exceptions to the adoption of open-source software but only with sufficient justifications. We recommend that such justifications be well-reasoned and recorded for public scrutiny.

B. **Principle 2** (Page 14)

Make reusable and shareable: Incorporate modular architecture to repurpose elements in diverse contexts. It helps in saving valuable time that would otherwise be wasted in reinventing the wheel for every separate build.

While it is important for architectures to be made reusable and shareable - these should be accompanied with a clear process for evaluating appropriate use and application to prevent misuse that could be associated with repurposing.

C. **Principle 4** (Page 15)

Ensure security and privacy: Apply 'Secure/ Privacy by design' principles, for e.g. E2E encryption, data purpose specifications, collection limitations

[13] https://meity.gov.in/writereaddata/files/policy_on_adoption_of_oss.pdf, pg. 3

[14] https://meity.gov.in/sites/upload_files/dit/files/Open_APIs_19May2015.pdf

[15] http://egovstandards.gov.in/sites/default/files/Policy%20on%20Open%20Standards%20for%20e-Governance.pdf

[16] https://static.mygov.in/rest/s3fs-public/mygov_158219311451553221.pdf, pg. 9

and user consent frameworks, etc. to ensure individual choice & privacy. Along with the choice to revoke access at any point in time, users should have control over how their data is used by the platform.

While this principle is strong by highlighting the importance of users having control over their data and emphasizing security, we feel it could be strengthened in the following ways:

- **Clarifying Ownership:** The principal can be strengthened if user rights over data-including ownership,monetization, and control are more clearly defined. Systems such as E-estonia that have been referenced by the white paper have made explicit efforts to ensure that data is controlled and owned by citizens and not the government.[17]

- **Need for express individual control over data sharing:** As per principle 1, a key element of the proposed framework of the NODE is the ability for various NODES to interact with each other and share data. Simultaneously, principle 4 allows for the ability of citizens to revoke access, and control data within a node but makes no express reference to the ability for citizens to authorize what data is shared between NODES and to what extent - prior to any actual data sharing taking place. Such a system is integral to ensuring data control of citizens within the E-Estonia system[18] referenced by the white paper. As such it must be made clear that individual approval will be required for every attempt to share data between Nodes or databases.

- **Lack of security standards:** The principle could be significantly strengthened by placing greater emphasis on key processes that work towards ensuring security including adherence to standards, breach notification, CVD, annual audits, and capacity building.

- N**ecessity and proportionality to define permitted use:** Though we appreciate that this principle recognizes the importance of privacy, it could be strengthened by emphasizing the need for clarity in permitted uses. We would recommend that defining permitted use is guided by the principles of necessity, proportionality, legitimacy, and legality.

[17] "In Estonia, everyone owns their data. It's not owned by the government. This was a fundamental and very important concept. It means I can give my data to the government and I can take it back. I decide who can look at my data and who cannot look at my data," - Linnar Viik, co-founder of Estonia's e-Governance Academy.
Mike Barlow and Cornelia Lévy-Bencheton, "The Smart Nation Where Everyone Owns Their Personal Data," *Smart Cities World* (blog), accessed March 20, 2020, https://www.smartcitiesworld.net/special-reports/special-reports/the-smart-nation-where-everyone-owns-their-personal-data.

[18]

II. Principles for Transparent Governance (6-10)[19]

A. Principle 8 (Page 18)

Create transparent data governance: Outline data policies & standards on ownership, contribution & consumption of data. Ensure that they are easily understood & readily available to all users. Put in place a set of mechanisms to enable enforcement of these and monitor adherence.

This principle could be further strengthened by explicitly noting the development of a mechanism for public reporting with respect to the use of the NODE and the results from any monitoring undertaken. The principle could also include a mechanism committing to continuous review and revision based on learnings from the monitoring and review.

B. Principle 9 (page 18)

Ensure the right capabilities: Nurture partnerships or ensure human resource policies and practices to attract and retain relevant talent from the private sector to supply skills such as analytics, customer support, technology development and maintenance, etc., required to build & operate the platform.

This principle could be strengthened by also committing to building capacity in relevant government departments and officials. The principle should also recognize the need for bringing in diverse backgrounds and skills including ethics and human rights.

C. Principle 10 (Page 19)

Adopt a suitable financing model: Create a sustainable financing model, which is aligned with the overall goals of the platform, to aid the right governance choices and ensure uninterrupted operations

Rather than simply noting the need for government adoption of "a sustainable financing model", it is imperative that the paper outline some of the options to be considered by the government and their limitations.

[19] Section 4.2, Pages 17-19
Ministry of Electronics and Information Technology Government of India, "Strategy for National Open Digital Ecosystem (NODE): Consultation White Paper," n.d., https://static.mygov.in/rest/s3fs-public/mygov_158219311451553221.pdf

While the government has made prior references to the monetisation of citizen's data through sale to the private sector[20], there is an absence of a regulatory framework that can be adopted by individual ministries so as to handle questions such as what model of monetisation can be adopted, what data can be monetised and the limitations of such monetisation.
It is also unclear how any monetisation going forward will be in compliance with the proposed Personal Data Protection Bill. For example, it is unclear whether data collected through NODES would be subject to use by the government and private entities in their creation of 'sandboxes' to facilitate technological advancement that favours the public good. While the state can monetise such a system, even if it is not directly monetised, the data in this instance is being used by the government to effectively subsidise R&D for specific private players.

We stress the need for the government to clearly outline a set of broad boundaries or red lines inside of which all monetisation models adopted by ministries and departments must operate. Such a guideline or set of rules must be the first step taken before considering any monetisation strategies.

III. Principles for a Vibrant Community (11 - 14)[21]

A. Principle 11 (Page 20)

Ensure inclusiveness: Incorporate user-friendly UI/UX design, omni-channel (e.g. web, mobile), universal, and affordable access. For example, ensure availability of content on the platform in all vernaculars spoken in the country (except only Hindi and English), create multiple formats of access to the services offered by the platform, such as IVRS services for users without smartphones. Support on-boarding and platform adoption.

This principle could be strengthened by committing to the following:

- **Broader scope of inclusivity:** Inclusiveness should not only be limited to the technical aspects of the software. Attention has to be

[20] Neha Alawadhi & Karan Choudhury, "Economic Survey Suggests Govt Can Monetise Citizen's Data as a Public Good," Business Standard India, July 4, 2019, https://www.business-standard.com/article/economy-policy/economic-survey-suggests-govt-can-monetise-citizen-s-data-as-a-public-good-119070401558_1.html.
Damini Nath, "Ministry Plans to Go from Open Platform to Eventual Monetisation of Cities' Data," The Hindu, September 11, 2019, sec. National, https://www.thehindu.com/news/national/ministry-plans-to-go-from-open-platform-to-eventual-monetisation-of-cities-data/article29385873.ece.

[21] Section 4.3, Pages 20-22
Ministry of Electronics and Information Technology Government of India, "Strategy for National Open Digital Ecosystem (NODE): Consultation White Paper," n.d., https://static.mygov.in/rest/s3fs-public/mygov_158219311451553221.pdf

paid to the secondary requirements that may be needed to access such a software. For example, if the software produced is dependent on or requires an Aadhar card for consumer operation, then it effectively excludes groups of people.

- **Accessible formats, platforms, technologies etc.** : The principle should specifically commit to adopting formats, standards, formats and technologies that enable accessibility to the differently abled. Previously, CIS has undertaken research into this area and provided comments on government policy and best practice.[22]

B. Principle 14 (Page 21)

Be analytics-driven and learn continuously: Build analytics as a central pillar to generate insights that enable improvements in platform performance, support robust policy-making and lead to the design of new solutions and services for users.

Furthermore, we would recommend that this principle include the following:

- **Accountability for the use of analytics:** As the development of NODE pertains primarily to public sector use - it will be important that algorithms meet a predetermined standard and that decisions informed by algorithms can be explained when necessary. These principles must be in line with the corpus of regulatory policy around the development of Artificial Intelligence (AI) in India and with the 'golden triangle' of fundamental rights-right to freedom of speech/expression; right to equality and the right to life-enshrined in the Indian Constitution.

C. Principle 15 (Page 22)

Enable grievance redressal: Define accessible and transparent mechanisms for grievance redressal, i.e. defined interfaces, processes and responsible entities, with a strong focus on actions for resolution.

We would recommend that this principle be placed under accountable governance frameworks.

Key components of a redress mechanism that should be brought into this principle include that the mechanism is: accessible, unbiased, provides protection to complainants, protects privacy, provides clear timeframes,

[22] The Centre for Internet and Society, "Accessibility," accessed March 31, 2020, https://cis-india.org/accessibility/blog/accessibility-blog.

has a clear and defined process, and has a mechanism for escalation. As discussed above, while it is beneficial to have a single point of contact that may enable individuals to engage with the grievance redressal mechanism, this single point is not sufficient. Therefore thought needs to be given to:

(a) **How national sectoral authorities** such as the Data Protection Authority or the Competition Commission of India fit into the NODE framework, and how grievances can be channelised to these authorities.

(b) **A clear definition of 'red lines'** outlining the scope of activities the NODE can undertake. The red lines should be designed with the intention of protecting fundamental human rights, as enshrined in The Constitution. Violation of red lines will need more urgent rectification and greater punishment channeled through a more centralised and formal grievance redressal mechanism, ideally a court.

3. Question 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. interdepartmental systems integration, legacy systems modernization, poor usability, and poor data quality)? How might these be overcome?

Challenges that may be faced in migrating to a NODE approach include:

1. Ensuring public interest and benefit in the use of the NODE
2. Ensuring security of systems, data and access
3. Ensuring accuracy of underlying data and enabling changes to data when necessary
4. Integrating into existing systems, frameworks, and policies
5. Migrating data that may be in different formats to a system dependent on specific formats
6. Ensuring the capacity of end users
7. Shifting from closed standards to open standards. An approach that could be considered is the 'comply or explain' method adopted in the Netherlands.[23]
8. Lack of adequate protection for rights
9. Ensuring meaningful redress of harms

[23] The Standardisation Forum, "A Guide for Government Organisations: Governance of Open Standards" (The Standardisation Forum, September 2011), https://www.forumstandaardisatie.nl/sites/bfs/files/atoms/files/Handreiking_Governance_of_Open_Standards.pdf.

4. Question 4

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

Please see comments under Principle 1

5. Question 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. [

First, the White Paper adopts a restrictive view on governance.Commonly accepted definitions of governance are much broader than the rules and laws described in the White Paper. As per the United Nations Development Project, governance is " *a system of values, policies and institutions by which a society manages its economic, political and social affairs through interactions within and among the state, civil society and private sector. It is the way society organizes itself to make and implement decisions – achieving mutual understanding, agreement and action. It comprises the mechanisms and processes for citizens and groups to articulate their interests, mediate their differences and exercise their legal rights and obligations. It is the rules, institutions and practices that set the limits and provide incentives for individuals, organizations and firms."*[24]

Therefore to adequately lay down the governance component of the NODE, the framework must identify:

1. Values, policies and institutions for
2. Making, implementing decisions, advancing mutual understanding and citizen participation and
3. Exercise legal rights and obligations.

As mentioned in the high-level comments, there should be a common governance frameworks and guidelines that draw from constitutional principles. These principles should then be adapted to specific scenarios and instances. We suggest that the common governance frameworks on the following topics make up the minimum core of values, rights and objectives that should be protected by the governance component of a NODE:

- Security
- Privacy - including end-user rights
- Protection of fundamental rights-right to freedom of expression, right to equality and right to life
- Openness
- Redress

[24] UNDP. 2007. Governance Indicators: A Users' Guide, 2nd ed., New York: United Nations Development Programme, p. 2.

- Transparency

6. Question 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.

Prior to providing an answer to this question, it is important to stress that any recommendations on the question of financing of NODEs is inherently limited due to the unclear nature of operational, regulatory and ownership standards for data under NODEs. Furthermore, it is also contingent on sector specific aspects such as the nature of data collected as well as the extent to which private players are active within the sector. Nonetheless, the following is a broad recommendation that can be used as a starting point by any ministry or department looking to develop a financing strategy for a NODE.

We believe that a multitude of financing options are available to ministries looking to implement NODEs. Importantly it is possible for NODEs to have multiple financing structures built into their structure at various levels.

At the base technological level we recommend that ministries and departments adopt a financing model that provides for greater government control so as to ensure the public nature of any technology produced. We recommend either a partial outsourcing or PPP framework wherein the government retains partial control of assets as well as control over overarching scope and regulatory framework of the project. However, it must be stressed that in both of these models, there cannot be a blanket recommendation for all NODEs. Rather a case by case approach must be taken to determine which of outsourcing, using existing government staff or hiring additional staff under government control is the most suitable strategy to follow[25]. Furthermore questions as to what form of outsourcing is to take place (General outsourcing, Transitional outsourcing, Business process outsourcing, Business benefit contracting[26]) must be answered on the basis of individual situations so as to strike a balance between innovative technological advancement and government control.

Following this we recommend that ministries and departments play an active role in monetisation efforts through indirect methods - that is through the ecosystem that the NODE looks to create. We recommend that governments adopt a private financing structure wherein infrastructure built on top of open source government technology is financed through private equity or debt. Concessions can be created between the government and such private entities outlining regulatory frameworks as well as potential

[25] Mahalik, Debendra. (2010). Outsourcing in e-Governance: A Multi Criteria Decision Making Approach. JOAAG JOAAG. 5.

[26] Millar, V. 1994. Outsourcing Trends, Proceedings of the Outsourcing, Cosourcing and Insourcing Conference, University of California - Berkeley

nominal monetary “licensing” terms. Revenue for private entities would be generated by end user fees[27].

With respect to crowdfunding[28], there is evidence to suggest that government involvement in private crowdfunding efforts creates a positive effect on consumer confidence and increased donation[29]. This must, however, be done in such a manner wherein government involvement not only increases the reach of the crowdfunding efforts but must also provide increased information to consumers while also acting as a form of accreditation of the proposed project. As such we recommend that such crowdfunding efforts be prioritised for experimental technology. We suggest that the government review proposals by private entities looking to be on the cutting edge of technology by building on top of the government’s open source technology/data, and back crowdfunding attempts by those proposals which are experimental in nature and have the potential to have massive positive impacts.

7. Question 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?

Though the paper recognizes that open and interoperable architectures are prone to misuse - it does not recognize the impact that such architectures can have on human rights. As discussed above, reference to the fundamental rights enshrined in The Constitution are essential to obtain a reasonable balance between public welfare and the protection of civil and political rights. At every point, a set of questions the principles of necessity, proportionality, legitimacy, and legality should guide decisions.

Based on learnings from research that CIS undertook on the use of big data and analytics in Governance[30] - some harms and challenges to consider that can result from open digital ecosystems include:

- Exclusion or loss of access because of technical failure, inaccurate information, or because of the information decisions are now based on.

[27] We recommend such a financing model in instances wherein the proposed private entity is working on creating a good or service that is not a public good or uniquely necessary for the functioning of the NODE ecosystem. This is so as to ensure that the profit motive does not necessarily undermine the accessibility of the NODEs core services.

[28] It is important to note that while crowdfunding often has a small scale image associated with it , we use this term to mean capital accumulation by companies through large investors as well.

[29] Sounman Hong and Jungmin Ryu, “Crowdfunding Public Projects: Collaborative Governance for Achieving Citizen Co-Funding of Public Goods,” *Government Information Quarterly* 36, no. 1 (January 1, 2019): 145–53, https://doi.org/10.1016/j.giq.2018.11.009.

[30] https://cis-india.org/internet-governance/blog/big-data-in-governance-in-india-case-studies

- Undefined downstream harms as a result of repurposing of data and architectures
- Inability to seek redress as a result of automation of services or technical failure
- Access to and use of data without consent
- Unauthorized access as a result of a security breach
- Vast digital profiles and lack of end user control
- Lack of alternative options for accessing services
- Monitoring
- Discrimination

10. Question 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.

Please see comment under principle 15

11. Question 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?**
- **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**
- **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?**
- **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. incentivising adoption, value sharing) and how you may overcome these?**

The nature of a NODE is such that its viability in a sector, technological architecture, governing framework and levels of community outreach will be dependent not only on the sector in which it is created, but also upon the specific service that the technology at the heart of it seeks to address.

With this in mind, rather than suggesting a hypothetical NODE that is limited to these constraints, CIS has proposed a set of frameworks that can serve as guides to any ministry or department looking to move from a GovTech 2.0 system to a GovTech 3.0 one.

These frameworks look at the viability of NODEs and their proposed structure, a broad set of universal regulations governing NODEs that must be applied by all ministries or departments, as well as a guide for assessing the impact of NODEs post implementation.

This framework can be found later in the report, under the section “The CIS guide on NODEs”

12. Question 12

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

13. Question 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?

As a research organisation, it is imperative that our analysis on the subject is informed through a multitude of sources - including but not limited to the examples provided in the question.

However another key tool would be direct communications with policy makers and regulators that will be looking to implement this transition to GovTech 3.0. Increased interaction directly with lawmakers will enable us to more effectively tackle research surrounding the specific questions that may arise from implementing this shift, thereby allowing us to provide better and more precise solutions to any such problems.

14. Question 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 through individual consultations and workshops and would recommend engagement with developers, public departments, and end users.

The CIS Guide on NODEs

As per the request of the Ministry of Electronics and Information Technology (MEITY), the Centre for Internet and Society has provided its feedback on the ministry's National Open Digital Ecosystem (NODE) consultation white paper.

As per our analysis of the paper - with specific reference to the examples of NODES provided as well as question 11 posed by the paper[31] - CIS has determined that there is a need for a clear framework to be developed that sets out a set of guidelines for all ministries or departments to follow in instances where they are looking to establish a NODE. Similar to the IndEA framework 1.0[32], such a framework for NODEs would look to create a unified set of metrics that can be used to determine whether a sector is currently ready for the implementation of a NODE, and if not, how can it be made more ready. It will also look to prescribe guiding rules on how a NODE must be structured accordingly.

This framework not only looks at the structure that a NODE should look to adopt, but also provides a universal governance framework that can serve as a basic minimum for all ministries and departments that are looking to develop standards of regulation and governance over NODEs.

However, given that NODE implementation has already begun in certain sectors, there is a need to go beyond a prescriptive framework for new NODEs. Accordingly, we have also developed a framework of analysis that looks to determine the relative success of a node vis a vis its output towards a specific goal and its adherence to the overarching principles outlined in the white paper. In doing so, it provides a common reference for the purposes of self evaluation and future improvement.

CIS has developed a tentative framework for doing exactly this. The framework adopts a holistic approach to understand the role that the NODE will play not only in terms of direct output within a ministry or department’s structure, but also its wider impact on citizens and private sector players. The following two annexes provide a general outline of the frameworks we have developed.

Considerations

This is currently a tentative framework and subject to change. We have focused on providing an overall picture of the framework in this document. Further research on the

[31] Page 36
Ministry of Electronics and Information Technology Government of India, “Strategy for National Open Digital Ecosystem (NODE): Consultation White Paper,” n.d., https://static.mygov.in/rest/s3fs-public/mygov_158219311451553221.pdf.

[32] Ministry of Electronics and Information Technology, “IndEA Framework (India Enterprise Architecture Framework)” (Government of India, October 2018), http://egovstandards.gov.in/sites/default/files/IndEA%20Framework%201.0.pdf.

topic will delve into the specific indicators that can be used to quantify each general metric mentioned in the framework. Such research will be made available to the public as well as the relevant ministry or department when ready.

Part 1 : Framework For Assessing Viability Of New Nodes

The underlying assumption present throughout the white paper is that the creation of NODEs would inherently improve the overall functioning of governance within a sector and have exponential positive benefits for citizens who are required to interact with the government. While this may be the case generally, the white paper does not propose a framework by which it is possible to assess the viability of a NODE within a sector, and what form a proposed NODE must take.

A. Viability Of A Node

I. Readiness Of A Sector For A Node

The first stage in the framework is an assessment of whether the field in question is one that is ready for a NODE and whether a NODE will lead to a real improvement on the ground.

We propose that the readiness of a sector for a NODE is dependent on the following factors:

1. History of Sector with regards to government digitisation:

   As outlined in the white paper[33] attempts by the government to digitise essential services have been underway since the turn of the century. The paper outlines 3 stages to this process:

   - GovTech 1.0 - Automation of government process and digitisation of records
   - GovTech 2.0 - E2E encryption, unified E gov portals, basic online data analysis
   - GovTech 3.0 - NODE based approach

   As such, the first stage in analysing the readiness of a sector for a NODE is mapping out the history of digitisation within that sector to determine at what of the above three stages the sector is currently positioned in. The success of NODES is dependent on pre existing digitisation efforts and the prior existence of digital infrastructure.

2. Existence of a thriving third parties/ private enterprises

   In its white paper[34] the government describes NODEs as systems that "enable different parts of the government system (across ministries and departments) to collaborate for service delivery and allow private players to build new services and solutions on top." A critical component therefore is the existence of considerable

[33] Section 3.1, Pages 3-5
Ministry of Electronics and Information Technology Government of India, "Strategy for National Open Digital Ecosystem (NODE): Consultation White Paper," n.d., https://static.mygov.in/rest/s3fs-public/mygov_158219311451553221.pdf.

[34] Ibid

private enterprises within the sector that are either providing an alternative to government services or are providing additional services in those areas wherein government systems do not have coverage.

While it is impossible to predict with complete certainty how business will react to the creation of a NODE within a sector (as it is entirely possible that the technological advancement will boost entrepreneurship within the sector), the prior existence of private entities is indicative of a gap between the needs of the consumer/citizen and the services provided by the government, and speaks to the potential of private sector growth and NODE technology adoption within that sector in the future.

3. Digital literacy, accessibility and penetration of target population

   Another important factor is the digital technology and access available to the target audience of the NODE[35]. The success of any NODE is largely dependent on the digital penetration of the population it aims to serve. This is not only a function of prima facie indicators of digital penetration such as number of smartphones in an area but also more underlying factors such as digital literacy, historical economic factors etc.

   It must be noted that the purpose of this point is not to discredit the creation of NODEs in areas with low digital pervasiveness - as NODEs can theoretically lead to increased digital adoption- but rather to highlight that any NODE or digitisation attempt in this sector must taken into account the facilities of end users.

II. **Prior Existence of a robust and certain policy framework protecting fundamental constitutional rights**

As discussed in our Comments to the White Paper,,a robust policy framework covering the following integral issues is a prerequisite before considering a NODE approach:

a. Clear classification of personal and non-personal data
b. Data producers' rights over data-including ownership and monetization
c. A Personal Data Protection Bill is passed giving the data principal rights over their data and guaranteeing their privacy.
d. Conceptualisation of non-personal data and how this conceptualisation fits into the NODE framework.

III. Scope of NODE

The scope of a NODE should be clearly outlined when the NODE is proposed to the relevant ministry/authority. An example of a clearly defined scope includes, " NODE for

[35] Section 3.1, Pages 3-5
Ministry of Electronics and Information Technology Government of India, "Strategy for National Open Digital Ecosystem (NODE): Consultation White Paper," n.d., https://static.mygov.in/rest/s3fs-public/mygov_158219311451553221.pdf.

assisting farmers make strategic decisions on planting crops through data-driven decision-making.” Example of an unclearly defined NODE includes “ NODE for undertaking sentiment analysis of population in X state for maintaining public order.”

IV. Cost/Benefit Of Proposed Node

The second stage of our framework is an analysis of the estimated cost to benefit ratio of moving from a GovTech 2.0 system to a GovTech 3.0[36] system. As such we propose the following metrics be examined when making this judgement.

1. Average Cost and ease of use of currently existing government systems within the field
   One of the most important factors in determining whether to adopt a NODE strategy within a sector, pertains to the cost of the NODE versus the ease with which the service the government aims to provide is accomplished offline. Once again, this is not to say an already easy procedure or readily available service cannot be made easier, simply that the government must take into account the cost to benefit ratio when making this decision.

2. Estimated Infrastructure Cost per user
   The second metric is the estimated yearly cost per user that would be accrued in creation and maintenance of a NODE. This metric must be analysed within the context of whatever form the technology or data at the heart of the proposed NODE will take.

V. Government Inertia

By government inertia we refer to the ease at which it is possible for a ministry or department to adopt large scale as well as quick technological change in order to implement digitization successfully. This metric primarily looks at the organizational structure of the ministry or department, ease of implementing change historically, existing ICT infrastructure, legal frameworks, financial and human resources etc. A ministry of department with a lower amount of inertia (that is to say with a higher amount of resources and ease of facilitating change) will find it significantly easier to overcome the hurdles that would arise in moving from a GovTech 2.0 system to a GovTech 3.0 system.

VI. National Factors

National level economic factors also play a role in determining whether a sector or state is ready for increased implementation of ICTs in the governance structure. Of these, GDP per capita has been seen to be the most salient of metrics to affect the development of

[36] Section 3.4, pages 10-12
Ministry of Electronics and Information Technology Government of India, “Strategy for National Open Digital Ecosystem (NODE): Consultation White Paper,” n.d., https://static.mygov.in/rest/s3fs-public/mygov_158219311451553221.pdf.

E-governance measures[37]. Other factors include overall societal literacy levels (beyond simply technological), private sector competitiveness, ICT adoption by private sector, urbanisation, etc.

B. What Form Should The Node Take?

The second stage of our framework consists of categorising the proposed NODE along the basis of a number of characteristics. These characteristics define the specific form that a NODE must take in terms of its technological, governance and community elements. These characteristics must be reflective of the purpose that the NODE aims to serve and in turn will affect any attempts at analysing said NODE - as NODEs that vary greatly in purpose and form cannot be judged by the same metrics.

Therefore, keeping in mind the nature of the sector and the purpose that the NODE aims to serve, we suggest that the following considerations must be kept in mind when determining the form of the NODE :

I. Delivery Platform

The government white paper[38] provides for a categorisation on the basis of the form that the delivery platform of the NODE will take. These include:

1. Modular applications
   These include technologies that have open APIs and which can be integrated into a host of third party services. Eg. eKYC

2. Data registries
   Singular sources wherein data of all actors within the sector can be made available

3. Stacks
   Combinations of applications, data registries and protocols. Eg. India Stack.

4. End User Solutions
   These usually constitute of a service/application layer along with the requisite UI on top of a stack

While this classification is useful in understanding the technological forms that various NODEs (or parts of a NODE) can take, we believe that this is an incomplete picture of the

[37] Bavec, C., Vintar, M.: What Matters in the Development of the E-Government in the EU? In: Wimmer, M.A., Scholl, J., Grönlund, Å. (eds.) EGOV 2007. LNCS, vol. 4656, pp. 424–435. Springer, Heidelberg (2007)
Singh, H., Das, A., Joseph, D.: Country-Level Determinants of E-Government Maturity. Communications of the Association for Information System 20, 632–648 (2007)

[38] Section 3.2.1, page 7
Ministry of Electronics and Information Technology Government of India, "Strategy for National Open Digital Ecosystem (NODE): Consultation White Paper," n.d., https://static.mygov.in/rest/s3fs-public/mygov_158219311451553221.pdf.

various structures that a NODE can adopt as it only tackles the structure of the NODE from the technological perspective. As such we recommend the following elements be considered under the categories of governance structure and community for all future NODEs. These factors are to be kept in mind when determining the structure of a NODE - so as to have a system that creates NODEs that have a clear and defined purpose and that are structured in a manner that serves that purpose and is proportional.

II. Governance Structure

The following elements have to do with governmental involvement in the NODE at various levels:

1. Ministry/ Department/ Institution responsible for the sector within which the NODE will function

   Questions relating to the administrative and regulatory structure in place within a norm would be specifically designed by the ministry of department in charge of overseeing the NODE[39]. As such the governance structure must be moulded so as to integrate successfully with the overseeing institution.

2. Extent of integration or reliance of NODE with other government systems outside of sector

   To that extent, it is entirely possible for a NODE to not only have significant overlap over multiple related sectors[40]. As such, any governance structure for the proposed NODE must take into consideration the sharing of power between the various ministries or departments under whose scope the NODE could come. Any such oversight structure would have to allocate regulatory power sharing between the ministries in such a manner that is proportional to

3. Proposed monetisation structure of NODE and role of private entities

   As mentioned in our comments on the white paper, we suggest that different NODEs adopt different financing models based on the delivery mechanism of the NODE, the sector and the specific level of the NODE (base technology, secondary applications, etc.)

III. Community

These characteristics have to do with the nature of the community that the NODE seeks to create and serve, and how it must be structured to best serve that community.

1. Nature of end user of NODE services - G2B, G2G, G2C

[39] “Each Ministry and State can use the ‘GovTech’ 3.0 approach to build NODEs”
Section 3.1, Page 4
Ministry of Electronics and Information Technology Government of India, “Strategy for National Open Digital Ecosystem (NODE): Consultation White Paper,” n.d., https://static.mygov.in/rest/s3fs-public/mygov_158219311451553221.pdf.

[40] Section 3.1, Page 4
Ministry of Electronics and Information Technology Government of India, “Strategy for National Open Digital Ecosystem (NODE): Consultation White Paper,” n.d., https://static.mygov.in/rest/s3fs-public/mygov_158219311451553221.pdf

The nature of the targeted end user, whether a citizen or a corporation, will alter the form that the NODE will take.

Part 2: Broad framework of 'Governance' for proposed NODEs

What is Governance?

Commonly accepted definitions of governance are much broader than the rules and laws described in the White Paper. As per the United Nations Development Project, governance is " *a system of values, policies and institutions by which a society manages its economic, political and social affairs through interactions within and among the state, civil society and private sector. It is the way society organizes itself to make and implement decisions – achieving mutual understanding, agreement and action. It comprises the mechanisms and processes for citizens and groups to articulate their interests, mediate their differences and exercise their legal rights and obligations. It is the rules, institutions and practices that set the limits and provide incentives for individuals, organizations and firms."*[41]

Therefore to adequately lay down the governance component of the NODE, the framework must identify:

4. Values, policies and institutions for
5. Making,implementing decisions, advancing mutual understanding and citizen participations and
6. Exercise legal rights and obligations.

India's Constitutional Edifice

India has a rich ethos of constitutional principles that guide and govern any project being undertaken for the purpose of public service delivery.The Indian Constitution not only protects fundamental civil liberties but also views the state as playing a 'transformative' role in the mitigation of structural inequality and empowering vulnerable communities.[42] The NODE consultation paper does not refer to any of these principles and thereby misses a key opportunity for devising a key governance framework. The golden triangle of fundamental rights-right to equality, right to freedom of speech and expression, and the right to life (that includes both procedural and substantive rights to due process) must be considered as key tools of governance. Further, as evolved in the groundbreaking *Puttaswamy* judgement, the Right to Privacy is one that can be derived from any or all of these fundamental rights. The protection of civil liberties can never be absolute but must always be balanced with other considerations-including the transformative role of The Constitution discussed above, and reasonable restrictions such as public order or national sovereignty.

Therefore when conceptualizing, designing, implementing and evaluating a NODE, the following questions need to be scrutinised by all three components of the NODE:

1.Is there a law allowing for the creation of the NODE?

[41] UNDP. 2007. Governance Indicators: A Users' Guide, 2nd ed., New York: United Nations Development Programme, p. 2.

[42] Gautam Bhatia, The Transformative Constitution: A Radical Biography in Nine Acts (Harper Collins,2019)

2. Is an intrusion into fundamental constitutional rights necessary, i.e. is it the least intrusive option available?
3. Is the intrusion proportionate to the objective (e.g. public service delivery) being sought to be objective? Is the objective legitimate?

Uniform framework for engaging with private sector

In a previous policy brief on Artificial Intelligence in the context of public -private partnerships, we had argued that all cases of public service delivery, primary accountability for the use of AI should lie with the government itself, which means that a cohesive and uniform framework which regulates these partnerships must be conceptualised.[43] This idea also applies to any NODE where a private sector from the 'community' is engaging in a public function.This framework should incorporate : (a) Uniformity in the wording and content of contracts that the government signs, (b) Imposition of obligations of transparency and accountability on the developer to ensure that the solutions developed are in conjunction with constitutional standards and (c) Continuous evaluation of private sector developers by the government and experts to ensure that they are complying with their obligations.

[43] https://cis-india.org/internet-governance/blog/ai-in-india-a-policy-agenda

Part 3: Framework For Analysing Existing Nodes

The third part of our framework looks to analyse the effectiveness of already existing NODEs. We do so by first analysing the effectiveness of the NODE in delivering systematic improvements at every level, and then contrasting that success with the extent to which these NODEs have adhered to the guiding principles outlined by the government.

The following framework is based on the principles outlined by MEITY in its white paper on NODEs, the reference models outlined in the IndEA framework 1.0 as well as third party research on e-governance analysis methodologies.

Multi Tiered Approach

While numerous methodologies regarding the analysis of e-governance exist, it has become apparent that following a singular approach leads to an incomplete picture of the impact of the system on citizens, government and businesses[44]. As such we propose that direct analysis of the impact of NODEs take a tiered approach - by examining the various levels of the NODE and its impact at said levels, we can have a holistic understanding of the impact that the NODE has had. We propose following a three tiered system of analysis to achieve this:

A. Analysis at the Technological Level

At the technological level, the metrics analysed look at the success of the technology in providing the service or achieving the scope of the project.

I. Success of Technology in meeting the Scope of the project

The first and most obvious factor to look at when determining the success of a NODE is the direct impact that the technology has had in increasing the total number of users who are availing of a government service.

II. Adherence to Principles outlined in the white paper guiding Delivery Platform Design[45]

In its white paper, the Ministry has outlined certain principles driving the technological design including openness, interoperability, modularity, reusability, sharable design, scalability, security and privacy. It is imperative to note that any analysis of such principles must not be done without firstly establishing the extent to which such principles are desirable within a specific NODE. That is to say, *these principles cannot be judged on a hypothetical minimum-maximum scale*. Rather, the extent to which each principle should manifest within the technological design of NODE must be determined

[44] Dalibor Stanimirovic et al., "Analysis of the Methodologies for Evaluation of E-Government Policies," in *Electronic Government*, ed. Hans J. Scholl et al., Lecture Notes in Computer Science (Berlin, Heidelberg: Springer, 2012), 234–45, https://doi.org/10.1007/978-3-642-33489-4_20.

[45] Section 4.1, Pages 14-16
Ministry of Electronics and Information Technology Government of India, "Strategy for National Open Digital Ecosystem (NODE): Consultation White Paper," n.d., https://static.mygov.in/rest/s3fs-public/mygov_158219311451553221.pdf

prior to any analysis of these principles - with the principles then being judged against this ‘optimal’ level.

1. <u>Openness</u>
   The first aspect to look at, at the technological level, is the extent to which the technology produced is in line with the principle of ‘openness’ outlined in the white paper. This would look at quantifying the ease with which such technology can be accessed, potential restrictions on which entities are allowed to access the technology and whether the technology is compatible with the tenants of FOSS.

2. <u>Interoperability</u>
   Interoperability looks at the ability of the technology or data to be used across multiple ministries/ departments, or in conjunction with other technologies and databases. An indicator of such would be the number of government services, technologies and databases whose functioning is linked in some way to the technology at the heart of the NODE.

3. <u>Modularity and Reusability</u>
   The ability of components of the technology to be used across a diverse range of situations so as to facilitate development of future technologies and solutions. This can be determined by looking how widely components of this technology have been used in the development of other technologies at the public and private level.

4. <u>Scalability</u>
   By contrasting the growth in user base with any corresponding drop in technological quality and access, it is possible to determine whether the technology is truly scalable in the Indian context.

5. <u>Security</u>
   Adherence to international security standards, built in security and redressal mechanisms, existence of a centralized institution in charge of maintaining and handling cases of security threats and breaches are some of the indicators that can determine the level of security that the technology possesses.

6. <u>Privacy</u>
   Unlike the previous factors, privacy is recognised as a right as per the constitution and as such is subject to a much stricter standard. Questions of privacy relate not only to the direct use of citizen data by a technology but also to issues of indirect use or sharing of data between ministries and departments. Furthermore, this must also include assessing design decisions that impact the ease with which users are able to enforce privacy on their end and effectively control their data.

B. <u>Analysis at the Organizational Level</u>

I. Changes to Organizational Structure of Ministries

Analysis at this level would look at the effect of the NODE on the structure of the ministry.

1. Vertical Integration within a ministry
   This includes any change within the organisational structure that has made it easier for various levels of the hierarchy to interact with each other as well as directly with the user.

2. Horizontal Integration with multiple ministries or departments
   While possible for a NODE to work in isolation, the white paper stresses the interoperability of the technology and data running these NODEs. Therefore, it is necessary to ascertain how the functioning of a NODE has impacted the structural relationship between the various ministries or departments involved in activities directly or indirectly relating to the NODE.

3. Changes in Human and Digital Resources
   Increased digital literacy of workforce, increased digital capacity and other such metrics provide a good indication on the impact of a NODE on a ministry's ability to be technologically competent going forward.

II. Adherence To White Paper Principles on Transparent Governance[46]

1. Government Transparency and Clear Rules of Engagement
   The success of a NODE can only be determined through an analysis of its impact on government transparency. The availability of clear guidelines relating to questions of
   of clarity on data ownership, regulatory standards, access and use of technology by third parties, monetisation strategies etc. all speak to this principle.

2. Proportionality of Measures
   The measures adopted on the technological and regulatory sides by the government must be proportionate to the specific service that the technology of the NODE aims to streamline or problem it aims to solve. This is to prevent the NODE from evolving beyond its intended scope.

3. Accountability of Institutions
   Existence of separate institutions whose purpose is to allow users to hold ministries or departments accountable for the regulation of NODEs is a must. This includes not only a legal framework for accountability but adequate capacity building in the form of new specialised institutions who will take up this task.

4. Financial Sustainability

[46] Section 4.2, Pages 17-19
Ministry of Electronics and Information Technology Government of India, "Strategy for National Open Digital Ecosystem (NODE): Consultation White Paper," n.d., https://static.mygov.in/rest/s3fs-public/mygov_158219311451553221.pdf

The final metric within this stage is the proposed financial model and its sustainability over time.

C. Analysis at the Socio Political Level

This metrics focus on societal response to the implementation of NODEs

I. Wider Impact on Society

1. Changes in Citizen Participation and Citizen Confidence
   One of the metrics by which it is possible to judge the success of the NODE's ability to foster a strong community is to monitor any changes in citizen participation with all services offered by the ministry or department in charge of the NODE.
   Another factor to be looked at is changes in the perception of citizens and users with respect to the process of availing of services from said ministry or department, i.e. increased citizen confidence in government run systems.

2. Impact on Rights of Citizens
   In conjunction with the earlier metrics on privacy, security, and proportionality, one of the key determinants of the success of a NODE is by analysing the impact that the NODE has on the rights of individuals. These rights include but are not limited to rights around privacy, freedom of expression, rights against discrimination, etc. Particular attention should be paid to the impact of a NODE on both the socio-economic and civil-political rights of vulnerable communities.

3. Economic Impact of NODE and Business Participation
   The success of the NODE is largely dependent on the wider impact of the technology or data produced by the government, and as such any analysis must incorporate the economic impact that has arisen from the development of such technology and its use by third party entities.

II. Adherence to White Paper Principles on fostering a vibrant community[47]

1. Inclusivity
   As mentioned in our response to question 1, there is a danger in the implementation of any new technology that either inherent biases or design flaws will lead to a situation wherein specific individuals or groups are de facto excluded from accessing the benefits of the technology. It is imperative that any NODE, in order to be successful, is not discriminatory in its execution and rather is wholly inclusive.

[47] Section 4.3, Pages 20-22
Ministry of Electronics and Information Technology Government of India, "Strategy for National Open Digital Ecosystem (NODE): Consultation White Paper," n.d., https://static.mygov.in/rest/s3fs-public/mygov_158219311451553221.pdf

2. Grievance Redressal
   This metric will look to analyse the availability of grievance redressal mechanisms to the end user. This refers not simply to the on paper availability of such mechanisms but also to the on the ground realities surrounding the accessibility and success of such redressal processes.

Conclusion

To reiterate, we believe that the current strategy regarding the shift from a GovTech 2.0 to a GovTech 3.0 or NODE system should be reassessed before taking any further steps. Our suggestion is guided by a number of reasons, primarily among which are:

- The absence of clear evaluation metrics at every stage of the NODE process - assessing viability, determining a framework of governance and ex post analysis of the impact of an implemented NODE.
- Lack of clear boundaries that define the scope of what a NODE is permitted to and not permitted to do
- A comparative and reliable appraisal of past efforts including Aadhaar and India Stack,
- Need for a clear and uniform policy prescription delineating personal data from non-personal data and a governance framework for both, and
- A lack of clear institutional mechanisms for redress and implementation.

CIS has attempted to address some of these concerns, including by providing a comprehensive framework for dealing with the first of these concerns. However, it is imperative that prior to moving forward with any steps, the government outline its proposed framework and strategy for dealing with the above mentioned issues.