Submission of BSA | The Software Alliance on the Draft National Digital Communications Policy 2018

CHAPTER 1: PREAMBLE

BSA | The Software Alliance ("**BSA**") welcomes this opportunity to comment on the Draft National Digital Communications Policy 2018 ("**Draft Policy**") that was issued for public consultation by the Department of Telecommunications, Ministry of Communications ("**DoT**") on Tuesday, May 1, 2018.

BSA is the leading advocate for the global software industry before governments and in the international marketplace. Our member companies are at the forefront of data-driven innovation, and they have a deep and longstanding commitment to protecting the privacy of personal information.

BSA's members include: Adobe, Amazon Web Services, ANSYS, Apple, Autodesk, AVEVA, Bentley Systems, Box, CA Technologies, Cisco, CNC/Mastercam, DataStax, DocuSign, IBM, Informatica, Intel, Microsoft, Okta, Oracle, salesforce.com, SAS Institute, Siemens PLM Software, Splunk, Symantec, The MathWorks, Trend Micro, Trimble Solutions Corporation, and Workday.

The Draft Policy has explored a wide range of issues, strategies, enablers and initiatives that are central to developing India's digital communications ecosystem.

BSA has extensive experience working with governments and other stakeholders around the world on policies that foster digital ecosystems. The input we offer through this submission focuses on the sections of the Draft Policy most relevant to the software industry.

Accordingly, we have provided specific responses to the following sections of the Draft Policy:

- Chapter 3, Section 1 – Connect India – 2022
- Chapter 4, Section 4 – Propel India Strategies – Harnessing Emerging Technologies
- Chapter 4, Section 7 – Propel India Strategies – Local Manufacturing
- Chapter 5, Section 2 – Secure India Strategies – Data Protection Regime
- Chapter 5, Section 4 – Secure India Strategies – Security of Digital Communications

We hope our submission herein and the information contained in our reference material is useful to the consultation process and will merit your kind consideration. We look forward to participating in this important discussion and stand ready to answer any questions you may have.

CHAPTER 3: CONNECT INDIA - CREATING A ROBUST DIGITAL COMMUNICATION INFRASTRUCTURE

Section 1 – Connect India – 2022

In Section 1 of Chapter 3 of the Draft Policy, the DoT enumerates specific targets to be achieved by 2022 in relation to India's broadband coverage. Further, it outlines certain initiatives to improve broadband access, such as the 'National Broadband Mission', 'Fiber First Initiative' and the 'National Digital Grid'.

BSA appreciates the DoT's commitment towards increasing broadband coverage and addressing existing challenges with respect to broadband deployment in India. We are also encouraged by the efforts of the DoT to introduce suitable regulatory, licensing, resource allocation and structural reforms designed to enhance India's digital infrastructure networks and accompanying regulatory framework.

For instance, the efforts to enable light-touch licensing and delicensing for the purposes of broadband proliferation, incentivizing and promoting the roll-out of fiber connectivity, or developing a unifying policy framework and spectrum management regime for broadband connectivity, are all key steps towards unlocking the potential of India's digital communications infrastructure.

BSA is encouraged by these initiatives, given their importance for the overall digital ecosystem in India. Digital economies require extensive, affordable broadband access, which in turn requires incentives for private sector investment in infrastructure and a regulatory environment that supports universal access.

Universal access to broadband, a robust fiber and digital infrastructure network and an effective spectrum management regime will allow individuals, companies, and government agencies to leverage various digital technologies – such as cloud computing – to promote growth and innovation throughout India.

In relation to the "Connect India" mission specifically, we would like to direct your attention to BSA's **2018 Global Cloud Computing Scorecard**[1] **("Cloud Scorecard")**, which includes a discussion on the issue of broadband deployment. As indicated in the report, India currently ranks 20th out of 24 leading IT economies in terms of its regulatory environment for cloud computing.

The lack of effective strategies with respect to broadband deployment puts India at risk of missing the economic benefits of the digital economy and contributed to India's lower ranking in the Cloud Scorecard vis-à-vis other countries. For further information in this regard, we wish to direct your kind attention to the **Country Report for India**[2] (see page 8 of the report).

Recommendation:

BSA welcomes efforts outlined in the Draft Policy to develop a 'Broadband Readiness Index for States and Union Territories' to help attract investments and address Right of Way challenges. We urge the Government of India to implement these and other initiatives to effectively increase broadband access.

[1] *See* BSA, 2018 Global Cloud Computing Scorecard, *at* http://cloudscorecard.bsa.org/2018/pdf/BSA_2018_Global_Cloud_Scorecard.pdf
[2] *See* BSA, 2018 Global Cloud Computing Scorecard – Country Report for India *at* http://cloudscorecard.bsa.org/2018/pdf/country_reports/2018_Country_Report_India.pdf

CHAPTER 4: PROPEL INDIA – ENABLING NEXT GENERATION TECHNOLOGIES AND SERVICES THROUGH INVESTMENTS, INNOVATION, INDIGENOUS MANUFACTURING AND IPR GENERATION

Section 4 – Propel India Strategies – Harnessing Emerging Technologies

In Section 4 of Chapter 4 of the Draft Policy, the DoT envisions a '*holistic and harmonized approach for harnessing emerging technologies',* including artificial intelligence ("**AI**"), cloud computing, and the Internet of Things, amongst others – a vision that BSA shares with the Government of India. As such, the Draft Policy appears to recognize the need to develop an enabling policy framework around a range of cutting-edge technologies that offer great promise to improve the lives of Indian citizens.

BSA member companies are leaders in the development of such emerging technologies and can offer unique insights into their tremendous potential. BSA has extensive experience working with governments and other stakeholders around the world on policies that promote an environment that allows the development and responsible adoption of these technologies.

BSA shares DoT's view expressed in the Preamble of the Draft Policy that India "stands poised to benefit from harnessing the new digital technologies and platforms". However, India will only be able to do so with a forward-looking, light-touch regulatory regime that balances security and the need for innovation, competition and investment. Today's and tomorrow's technologies should not be stifled by yesterday's regulations. Apropos, India needs a fresh look at their regulatory approach to reflect changes in technologies and markets. The future will require a more technology-agnostic and flexible approach.

To propel India forward in this 4th Industrial revolution, India must embrace policies to enable its economy to prosper in a world where productivity, innovation, and efficiency will increasingly depend on reliable, mobile, and ubiquitous access to powerful, cloud-based information and information processing capabilities. BSA encourages DoT to develop a balanced regulatory framework that will ensure the future growth of new and emerging data services.

The Policy must promote a regulatory regime that minimizes the amount of complex regulatory permissions needed to invest and innovate, is future proof, forward looking and sufficiently flexible to adapt to new technologies, new services and platforms, while embracing international best practices.

Accordingly, in order to facilitate the process of developing an enabling regulatory environment for emerging technologies in India, we share the views below to contribute to the Government of India's efforts to create a policy landscape that will allow these technologies to further promote societal and economic benefits in the country.

- **Artificial Intelligence:**

  We present a number of insights that will help support the DoT in its efforts to develop a roadmap around artificial intelligence ("**AI**"). Our primer on Understanding AI[3] contains an overview of the nature of AI, as well as potential use-cases.

  In our AI Policy Overview[4] and connected issue snapshots**,** BSA has identified five key pillars for facilitating responsible AI innovation – (1) Building Confidence and Trust in AI Systems; (2) Sound Data Innovation Policy; (3) Cybersecurity and Privacy Protection; (4) Research and Development; and (5) Workforce Development.

  Finally, we wish to point you towards research prepared by Software.org, the BSA Foundation, which is an independent and nonpartisan international research organization. **Software.org's report on Artificial Intelligence[5]** discusses the necessary policy initiatives

[3] *See* BSA, Understanding AI *at* http://www.bsa.org/~/media/Files/Policy/BSA_2017UnderstandingAI.pdf
[4] *See* BSA, AI Policy Overview *at* http://www.bsa.org/~/media/Files/Policy/BSA_2018_AI_PolicyOverview.pdf
[5] *See* Software.org, Report on Artificial Intelligence *at* https://software.org/wp-content/uploads/AI_Report.pdf

required to maximize the benefits of AI and may be useful in the DoT's formulation of a holistic approach to AI for the digital communications sector.

- **Cloud Computing:**

BSA has participated extensively in policy discussions around cloud computing in India, including the recent consultation process concluded by the Telecom Regulatory Authority of India (**"TRAI"**) on cloud computing.

In relation to the application of cloud computing to the digital communications sector, we would like to direct your attention to the abovementioned **2018 BSA Global Cloud Computing Scorecard**[6], which remains the only global report to rank countries' preparedness for the adoption and growth of cloud services. **India's country report** may be found therein[7], which highlights opportunities for improvements in data privacy & IT readiness, amongst other considerations.

Specifically on the Draft Policy, BSA strongly supports the DoT's strategy to enable *'a light touch regulation for the proliferation of cloud based systems'* under sub-section (f) of this Section. We find that this is also in line with a key recommendation made by the TRAI emerging out of the aforementioned consultation process on cloud computing[8].

However, the current language of this strategy may be viewed in a narrow light, to suggest that a 'light touch approach' should only apply to the *proliferation* of cloud-based systems, and not to cloud computing or cloud services in general – which was the broader approach favored by the TRAI and supported by BSA as well.

Therefore, we suggest that this strategy be suitably revised to state the following- '*enabling a light touch approach towards the proliferation, development and regulation of cloud-based systems and services'*

BSA is encouraged by the Draft Policy's focus on improving India's broadband architecture and fiber connectivity networks, including specific strategies to eliminate infrastructural and regulatory barriers. These represent critical steps towards creating a strong foundation for the adoption and growth of cloud services in India.

In this regard, we recommend that the DoT look towards incentives for greater private participation among various stakeholders, including cloud service providers, in the development of India's network and infrastructural capabilities.

In creating these initiatives, we encourage DoT to avoid preferences that may restrict market access, impose technical standards that diverge from widely adopted global standards, or grant special incentives, subsidies or tax benefits that are not available for foreign providers. Such preferences and incentives would reduce the Indian economy's access to cutting edge global technologies and services and increase costs.

- **Internet of Things:**

The world is on the verge of another wave of technological advancement fueled by a vast sea of connected devices. At the core of the 'Internet of Things' revolution will be powerful computers, ubiquitous connectivity, low-cost sensors and transformative cloud analytics engines.

---

[6] [6] *See* BSA, 2018 Global Cloud Computing Scorecard, *at* http://cloudscorecard.bsa.org/2018/pdf/BSA_2018_Global_Cloud_Scorecard.pdf
[7] *See* BSA, 2018 Global Cloud Computing Scorecard – Country Report for India *at* http://cloudscorecard.bsa.org/2018/pdf/country_reports/2018_Country_Report_India.pdf
[8] *See* TRAI, Recommendations on Cloud Services *at* https://trai.gov.in/sites/default/files/Recommendations_cloud_computing_16082017.pdf

In this regard, we would like to direct your attention to the **Software.org report titled 'Sensor Sensibility: Getting the Most from the Internet of Things**'[9], which examines the emerging trends in IoT and machine-to-machine technologies, along with specific applications and challenges to realize the full potential of this transformative technology.

In response to the Draft Policy, we would like to direct your attention specifically to Page 5 of the report, which outlines three aspects that we think governments should consider in developing the IoT ecosystem, namely relating to investments and R&D, technology mandates around software and hardware development and industry partnerships to improve security.

- **Blockchain:**

Though 'blockchain' technology is not specifically mentioned within the Draft Policy, we recommend that DoT consider its potential application in the digital communications sector as it represents a powerful foundational technology with incredible socio-economic benefits. For further insights on this technology and its potential applications, the DoT may consider **Software.org's primer on Understanding Blockchain[10].**

Impact of Data Localization on Emerging Technologies

We would like to specifically respond to Section 2.2(f) of the Draft Policy, which envisages establishing India as a "*global hub for cloud computing, content hosting and delivery, and data communication systems and services*."

Given the context in which this strategy has been outlined in the Draft Policy, i.e. the need to harness emerging technologies like AI, Cloud Computing, Big Data, IoT, etc., we would like to submit for your kind consideration, the potential negative effects of any server or data localization requirements for India's digital ecosystem and how it might curtail its ability to participate in the global digital economy.

Firstly, the seamless transfer of data across international borders is critical to cloud computing, data analytics, and other modern and emerging technologies and services that underpin global economic growth. In fact, the recent **White Paper published by the Expert Committee on Data Protection[11]** acknowledges that "the ability to move data rapidly and globally has been a key building block of the global economic order." Enabling cross border data flows and refraining from implementing data and infrastructure localization policies as a condition for operating in the market, will encourage investment and help innovation prosper in India.

Second, data localization requirements may have a detrimental impact on global efforts to safeguard individual privacy and security. The data-driven businesses of today have established systems and processes designed to protect the privacy and security of personal information. Some of these businesses, including BSA member companies, operate simultaneously in different sectors and industries and across different jurisdictions. Server or data localization requirements have the potential to introduce vulnerabilities into otherwise secure global networks because such requirements create additional entry points into global information security platforms. Furthermore, the security of data itself is not a function of where it is stored, but more so of the processes put in place to secure the redundancy, confidentiality, availability, and integrity, of data. It is thus well known that storing data in the cloud with its many layers of security and access locks provides the best option to ensure privacy and security of citizen data as well as control.

Third, and notably, data analytics, relying on cross-border data flows, have contributed significantly to the social good, including enhancing public health and safety. For example, researchers around the world leverage data analytics to respond to natural disasters, including in the wake of the 2015

[9] *See* Software.org, Sensor Sensibility: Getting the most out of the Internet of Things, *at* https://software.org/wp-content/uploads/iot-sensor-sensibility.pdf#page=6
[10] *See* Software.org, Understanding Blockchain *at* https://software.org/reports/blockchainprimer/
[11] *See* Committee of Experts under the chairmanship of Justice B.N. Srikrishna, White Paper on Data Protection *at* http://meity.gov.in/writereaddata/files/white_paper_on_data_protection_in_india_18122017_final_v2.1.pdf

earthquake in Nepal, where they conducted a real-time analysis of mobile phone patterns to assist in disaster relief efforts. In this regard, we would like to direct your attention to **BSA's report on cross-border data flows**[12], especially Page 4 of the report, which discusses the importance of cross-border data flows to harness the technologies of the future, including the specific technologies discussed in the Draft Policy, such as Artificial Intelligence and Big Data Analytics.

Lastly, it is important that the DoT consider the global ramifications of any particular strategy, given its long-term vision of establishing India as a 'global hub' for data communication systems and services. Any effort to impose data or server localization requirements in India could be replicated in other parts of the world, which would result in data silos in different countries, and would run counter to the vision outlined in the Draft Policy of making India a 'global hub' for data services.

Recommendation:

All these emerging technologies remain in a relatively early stage of development. In some areas, limited government regulations are appropriate – for example, to establish balanced data privacy frameworks.

In such cases, it is important for the Government of India to keep such regulations in line with emerging international trends and best practices. We urge the Government of India to refrain from adopting an overly-regulated approach that would likely inhibit innovation, as well as the development, deployment, and growth of these emerging technologies to the detriment of the vision of the Draft Policy for India.

[12] *See* BSA, Report on Cross Border Data Flows *at* http://www.bsa.org/~/media/Files/Policy/BSA_2017CrossBorderDataFlows

CHAPTER 4: PROPEL INDIA – ENABLING NEXT GENERATION TECHNOLOGIES AND SERVICES THROUGH INVESTMENTS, INNOVATION, INDIGENOUS MANUFACTURING AND IPR GENERATION

Section 7 – Propel India Strategies – Local Manufacturing

On page 15, the Draft Policy seeks to impose preferential market access requirements by stating that in public procurement practices, especially relating to security products, there should be a preference for '*domestic products and services with domestically owned IPR*'.

We are concerned that efforts to implement any preferential market access requirements will undermine the vision of the Draft Policy to 'secure India' for the following reasons:

(a) The Draft Policy must consider prevailing market conditions:

Today, the research and development (**"R&D"**) of information technology ("**IT**") and cybersecurity products, services, and solutions is often global, drawing on researchers in disparate geographies to develop integrated solutions. As a result, intellectual property **("IP")** is not typically localized. Therefore, basing requirements on whether a particular entity, based in a particular jurisdiction owns or controls IP is not practical and negatively impact innovation.

As such, the Draft Policy does not acknowledge the increasingly global nature of R&D. This may result in confusion for procuring agencies, especially in cases where domestic products and services are integrated with global security or other solutions. This could have a detrimental impact on the market for such products and services in India.

(b) The Draft Policy should promote cyber resilience:

In a fast-paced environment where malicious actors are finding new ways to launch attacks on critical infrastructure, governments should ensure that procuring agencies are encouraged to acquire cutting-edge, world-class cybersecurity technologies available in the global market which can be deployed immediately.

Accordingly, IT and security products should be evaluated on the basis of the extent to which they improve resilience and their capacity to defend against malicious attacks, and not on the basis of the country of origin.

The Draft Policy also runs counter to the spirit of the Framework for the US-India Cyber Relationship ("**US-India Cyber Framework**"), adopted June of 2016. The "Shared Principles" of the Framework include a commitment to *"to support the development and use of international standards and best practices for technology products and services"* and *"promote cooperation between and among the private sector and government authorities on cybercrime and cybersecurity."*

By seeking to adopt a procurement framework that emphasizes the country of development and manufacture, rather than product quality, the implementation of preferential market access conditions in the Draft Policy runs counter to the objectives of the Government of India to achieve cyber resilience and those set out in the US-India Cyber Framework.

(c) The Draft Policy should incentivize further investment in cybersecurity:

The Draft Policy should create an environment for companies to increase the investment in utilizing and creating the best global IT and security solutions for use in India.

The Draft Policy runs counter to this focus, and to the overall objective to 'secure India', by encouraging private operators and requiring government agencies to focus on a limited set of solutions based on a combination of IP ownership considerations and local sourcing and procurement mandates.

Such an effort will likely increase risks in the short-term with no or little contribution to improving security in the long-term.

Recommendation:

BSA recommends that government agencies and private operators focus on procuring products and software that are developed in accordance with international IT and cybersecurity standards, rather than on where the products and software were developed or manufactured, or whether IP is owned or controlled locally.

By adhering to standards that are global and developed through a multi-stakeholder process, India can ensure the protection of technology users and of national security, whilst driving innovation and investment in India. This approach is critical to security as deviation from standards that are globally developed could introduce vulnerabilities, undermine multilateral collaboration to confront transnational cybersecurity threats, and impact the interoperability of tested security features. Although India is a unique country with its own challenges, adhering to international norms and technical standards is the most effective, efficient and competitive avenue for achieving DoT's important objectives.

Accordingly, we urge India to refrain from preferences that may disadvantage global service providers by restricting market access, imposing technical standards that diverge from widely adopted global standards, or granting special incentives, subsidies or tax benefits that are not available for foreign providers. Such preferences and incentives will reduce the Indian economy's access to cutting edge global technologies and services, increase costs, and make it harder for domestic Indian software developers and service providers to expand to international markets.

Further, BSA encourages the Government of India to closely engage with the private sector before adopting any policies that would have a significant impact on the software and IT ecosystem in India and around the world.

CHAPTER 5: SECURE INDIA – ENSURING DIGITAL SOVEREIGNTY, SAFETY AND SECURITY OF DIGITAL COMMUNICATIONS

Section 2 – Secure India Strategies – Data Protection Regime

Firstly, we would like to state that we share the DoT's vision for establishing a *'strong, flexible and robust Data Protection Regime',* as outlined in Section 2 of Chapter 5 of the Draft Policy.

As a global organization, we actively follow privacy and personal data protection developments around the world. We have consistently highlighted that an effective personal data protection regime provides appropriate protections for individuals' personal data while also spurring innovation that is fueling the global economy.

Accordingly, we commend the DoT's focus, as outlined in the Draft Policy, to ensure that core data protection and security principles are applied and enforced in the digital communications sector.

In our past submissions to public consultation processes initiated by the Government of India, we have provided detailed inputs on the necessary steps required to advance this vision for India's digital ecosystem. We urge the DoT to consider the issues discussed therein, while identifying the initiatives required to achieve the objectives contained in this Section.

Accordingly, for your kind reference, we wish to direct your attention to the following:

1. BSA Personal Data Protection Principles[13]**:** Our Personal Data Protection Principles seek to guide policy makers around the world towards developing effective regimes for privacy and data protection. The Principles rest on five pillars of data protection: (1) Scope and Definition of Personal Data; (2) Collection, Use, Processing and Disclosure of Personal Data; (3) Allocation of Obligations and Liability; (4) International Data Transfers; and (5) Personal Data Breach Notifications.

2. BSA Submission to the White Paper of the Committee of Experts on a Data Protection Framework for India[14]**:** In July 2017, the Government of India constituted a Committee of Experts to deliberate on a data protection framework for India under the Chairmanship of Justice B.N. Srikrishna ("**Expert Committee**"). The Expert Committee released a White Paper in November 2017, seeking detailed inputs from the public on the protection of data in India. BSA contributed to this process, responding to a number of specific issues raised by the White Paper.

3. BSA Submission on TRAI Consultation Paper on Privacy, Security and Ownership of the Data in the Telecom Sector[15]: In August 2017, the TRAI released a Consultation Paper seeking detailed inputs from the public on the protection of data in the telecom sector. BSA also contributed to this process, responding to a number of specific issues raised by the Consultation Paper.

Key Points for India's Data Protection Regime

Amongst other elements, our inputs consistently emphasize the following key points:

- The definition of personal data should apply to information that is reasonably linked to an identified or identifiable individual;

[13] *See* BSA's Personal Data Protection Principles *at* http://www.bsa.org/~/media/Files/Policy/BSA_2018PersonalDataProtectionPrinciples.pdf
[14] *See* BSA Submission to White Paper of Committee of Experts on a Data Protection Framework for India *at* http://www.bsa.org/~/media/Files/Policy/Data/012918BSAResponseofWhitePaperDataPortectionFrameworkIndia.pdf
[15] *See* BSA Submission on TRAI Consultation Paper on Privacy, Security and Ownership of Data in the Telecom Sector *at* https://trai.gov.in/sites/default/files/BSA_07_11_2017.pdf

- A risk-based approach should be used to determine whether heightened protections should apply to sensitive data based on the context in which data is used;
- The law should clearly define data controllers and processors;
- The law should provide appropriate and flexible bases for processing data;
- The law should adopt a flexible approach to notice and consent;
- The law should facilitate international data transfers and avoid burdensome restrictions, such as data localization requirements;
- The framework should embrace the principle of accountability; and
- Personal data breach notification requirements should apply where there is a material risk of harm to individuals.

Recommendation:

BSA is closely following the efforts of different regulators and Ministries to develop a robust data protection regime in India to protect data across sectors and the ecosystem as a whole.

However, given that a comprehensive privacy and data protection law for India is yet to be formulated, we urge the DoT to coordinate with other sectoral regulators and the Expert Committee to ensure that the various policy processes involving data protection across the Government of India are harmonized.

This will ensure that various sector-specific efforts, as well as broader initiatives such as the Draft Policy, can be tied together to create a holistic data protection framework that can secure India's digital communications networks and the larger digital ecosystem.

CHAPTER 5: SECURE INDIA – ENSURING DIGITAL SOVEREIGNTY, SAFETY AND SECURITY OF DIGITAL COMMUNICATIONS

Section 4 – Secure India Strategies – Security of Digital Communications

We appreciate the DoT's efforts to ensure that cybersecurity occupies a top priority in the Draft Policy.

BSA views strong and smart cybersecurity policy as a critical ingredient to the stability of the Internet and the vibrancy of the global economy. We recognize that governments around the world confront an increasingly complex and diverse array of cybersecurity threats, and that identifying the most effective policy approaches to defend against cybersecurity is a top challenge.

As this Section indicates, the Draft Policy envisions a comprehensive, holistic, and layered approach towards cybersecurity, with the intent of creating a strong foundation for defending against malicious cyber actors, and taking full advantage of the opportunities of the digital economy.

To assist the DoT in advancing these objectives, we urge the DoT to consider **BSA's International Cybersecurity Policy Framework**[16] ("**Cybersecurity Framework**").

Our Cybersecurity Framework provides a model for a comprehensive national cybersecurity policy. It is intended to serve as a tool both for policymakers considering foundational cybersecurity legislation and for those examining gaps and shortfalls in existing policies.

Recommendation:

The Cybersecurity Framework recommends that cybersecurity policies be formulated on the basis of six overarching principles:

1. Policies should be aligned with internationally recognized technical standards.
2. Policies should be risk-based, outcome-focused, and technology neutral.
3. Policies should rely on market-driven mechanisms where possible.
4. Policies should be flexible and adaptable to encourage innovation.
5. Policies should be rooted in public-private cooperation.
6. Policies should be oriented to protect privacy.

Rooted in these principles, the Cybersecurity Framework outlines a comprehensive foundation for cybersecurity policy, including detailed principles to guide legislative and administrative action.

In section 3.3(e), the Draft Policy sets out a goal to formulate a policy on 'encryption and data retention', based on global standards. BSA strongly recommends that all stakeholders in the ecosystem push for strong encryption in an effort to safeguard individuals' security and privacy and to prevent criminals and terrorists from compromising digital infrastructure. In this regard, we would like to direct your attention to **BSA's Encryption Principles**[17], which sets out 8 key principles to evaluate any proposed legislation, regulation or policy on encryption, as follows:

1. Whether it improves data security
2. Whether it enhances law enforcement and counter-terrorism capabilities

[16] *See* BSA's International Cybersecurity Policy Framework *at* https://bsacybersecurity.bsa.org/wp-content/uploads/2018/04/BSA_cybersecurity-policy.pdf
[17] *See* BSA's Encryption Principles *at* http://encryption.bsa.org/downloads/BSA_encryptionprinciples.pdf

3. Whether it promotes privacy
4. Whether it protects confidential government information
5. Whether it encourages innovation
6. Whether it helps defend critical infrastructure
7. Whether it recognizes and understands the global impact of such policies
8. Whether it promotes transparency in the policy formulation process

CONCLUSION

BSA thanks the DoT for this opportunity to offer comments on India's proposed policy framework for building *a 'ubiquitous, resilient, secure and affordable*' digital communications network in India.

We hope our submissions are useful to the consultation process and will merit your kind consideration. We look forward to participating in this important discussion and stand ready to answer any questions you may have.

Regards,

Venkatesh Krishnamoorthy
Country Manager - India
BSA | The Software Alliance

E-Mail: venkateshk@bsa.org