24 January 2019

H.E. U Thar Oo
Deputy Minister
Ministry of Transport and Communications (MOTC)
Government of Myanmar

Subject: Submission for Industry participation in the development of digital economy laws in Myanmar - Cybersecurity Law, E-Commerce Law, and Data Protection Law

Dear Deputy Minister,

The Asia Internet Coalition (AIC) and its members express our sincere gratitude to the Ministry of Transport and Communications and the Government of Myanmar for this opportunity to submit this letter requesting for wider industry participation in the development of the cybersecurity, data protection and e-commerce laws in Myanmar. AIC is an industry association comprised of leading Internet and technology companies and seeks to promote the understanding and resolution of Internet, ICT, and cybersecurity policy issues in the Asia Pacific region. Our member companies would like to assure the government that they will continue to actively contribute to the security of digital platforms, products and services in support of the digital economy goals of Myanmar.

This input is a follow up to the bilateral meeting that you led at TELMIN 2018 with US ASEAN Business Council, where your delegation graciously agreed to receive inputs from US industry groups.

We commend the Ministry of Transport and Communications and the Government of Myanmar for commencing the drafting of essential laws in context of Myanmar's digital economy development. We support these efforts to develop a legal framework for cyber and information security, that will help boost technology adoption across sectors – payments and financial services, health and life sciences, transportation and logistics, and e-commerce – where continued development and investment are necessary for Myanmar to stay competitive and continue its rapid upward economic trajectory.

With a digital revolution that is profoundly transforming our societies, development of a legal framework favoring such transformation is essential and should take into account the inputs of stakeholders. We urge that the ministry engage with local and recognized international experts to shape the contours of the legal frameworks in accordance with accepted global standards to ensure the safe use of social media, and the protection of data and networks. We further suggest that the government consider an industry level multi-stakeholder approach towards the development of aforementioned laws, provision of which is to ensure Myanmar remains a vibrant economy. This should involve experience, knowledge and expertise of the public and private sectors, academia and civil society.

As such, please find attached to this letter an **appendix** with a detailed set of initial comments that we encourage the ministry to review, as good practices while framing rules and regulations. Importantly, we also request the ministry to hold a transparent, multi-stakeholder approach in developing the laws, and we will appreciate the opportunity to engage in a dialogue with the ministry and the government in general to serve as a useful collaborative platform in designing the regulatory framework in Myanmar.

In accordance to the objective of this letter, we respectfully request that the ministry consider this submission for further dialogue. Should you have any questions or need clarification please do not hesitate to contact us directly at Secretariat@aicasia.org or +65 8739 1490. Thank you for your time and consideration.

Sincerely,

Jeff Paine
Managing Director
Asia Internet Coalition (AIC)

Cc.:

- U Soe Thein, Permanent Secretary, Ministry of Transport and Communications (MOTC)
- U Than Htun Aung, Director International Affairs, PTD and Project Director, Telecom Sector Reform Project
- U Sai Saw Lin Tun, Deputy Director General, Department of Information Technology and Cyber Security

Enclosure

APPENDIX

I. CYBERSECURITY

Cybersecurity is a fundamental factor in achieving socio-economic development, and it is imperative to instigate strategic thinking and help national leaders and policymakers to develop, establish and implement national cybersecurity strategies. Cybersecurity is a complex challenge that encompasses different governance, policy, operational, technical and legal aspects and should be based on overarching principles and good practice that should be considered in the process of drafting, developing and managing a national cybersecurity legislation. Priorities for national cybersecurity strategies vary by country, so while the focus for one country may be addressing critical infrastructure-related risks, for others it may be protecting intellectual property, promoting trust in the online environment, or improving cybersecurity awareness of the general public; or a combination of these issues. Therefore, the government should look at cybersecurity holistically across their digital ecosystem. In this vein, developing a cybersecurity law requires coordination across the international community on cybersecurity capacity-building to execute defensive responses to cyber-threats, entailing cyber-preparedness, response and resilience, and building confidence and security.

Contours of a cybersecurity framework

A national cybersecurity strategy typically takes the form of a framework that outlines a vision and articulates local priorities and principles. The most important strategies are (i) embedded in living documents that are kept up to date and developed in partnership with public and private stakeholders (ii) based on clearly articulated principles that reflect values and traditions (iii) based on a risk management approach where public and private sector partners agree on the risks that must be mitigated and managed.

While, there is no single one size fits all model for a nodal agency, successful approaches however exhibit the following core characteristics:

- A focus on establishing a single national cybersecurity authority;
- The provision of a clear mandate to the agency;
- Ensuring the agency has appropriate statutory power;
- An organizational structure incorporating functions around policy and planning, outreach and partnership, communications, operations, regulatory and compliance; and
- An ability to evolve and adapt as technology develops.

Any regulation that is introduced should also be based on a thorough understanding of the threats, vulnerabilities and potential consequences facing the country. In adopting a risk-based approach, governments will recognize that all activities involve some degree of risk and that no organization has unlimited resources to apply to security. The approach will also allow governments to prioritize their security investments on the most important national assets.

Roadmap to creating a cyber security strategy

All societies and governments are vulnerable to attack in the cyberspace due to the growing interconnectedness of networks, 'internet of things' such as machines, sensors, e-commerce, and explosion of data through multitude of internet connected devices. Solutions and responses to cyber threats need to be holistic and should address different scenarios in developing a robust cybersecurity strategy with a reference to the framework below:

a. Awareness and Public Education

The responsibility of maintaining safe and secure Internet and networks rests with all segments of society, and it is important that all users of ICT play their part in the defence against cyber threats and cyber-attacks. It is through cooperation between government, consumers, small- and medium-sized businesses (SMBs), enterprises, contractors, security vendors, IT industry and the cybersecurity research community that networks and devices can be resilient enough against threats and attacks. In order to do this, governments should launch and fund programs to raise awareness among all stakeholders on cyber-security. As an important step, schools and universities could develop curriculums that integrate ICT use and cyber security into courses. Alongside this, individuals operating ICT systems both in the public and private sector should be given expert training on managing the risks associated with their jobs.

b. Readiness – Crisis Management Plan

It is important for government agencies to work in close collaboration and exchange information, first at the national level, and second at the regional and international levels. Ministries and regulators need to be part of a national cyber strategy planning process. The Strategy should call for the establishment of appropriate national incident- response capabilities to address operational cybersecurity challenges. Often, this capability refers to the establishment of Computer Emergency Response Teams (CERTs), Computer Security Incident Response Teams (CSIRTs) or Computer Incident Response Teams (CIRTs) with national responsibility. Although the specific organisational form of a CERT/CSIRT/CIRT may vary (e.g., national, government, sectoral, etc.), and not every country may have the same needs and resources, these specialised and dedicated teams should provide a set of both proactive and reactive functions, as well as preventive and educational services. Despite Myanmar having a provision of CERT mechanism, it is relatively less effective and under-resourced. Therefore it is important that the existing CERT is strengthened, in a way that follows best practice. For example, US-CERT is the 24x7 operational arm of the Department of Homeland Security.

c. Prevention – Safe and Protected Network Infrastructure

Many attacks can be prevented by following practices such as installing firewalls, being attentive to security updates, monitoring enterprise end-user software installations, using up-to-date anti-malware tools, and adhering to good security practices and IT policies. Techniques such as application whitelisting, where only trusted programs are enabled, and browser security can also help. But the best prevention is simply to use genuine, current and up-to-date software. This means procuring computers and software from trusted sources, ensure legal software usage, and following activation and registration protocols to benefit from IT support. Poor procurement practices can bring unsolicited malware or outdated software into the system which can in turn lead to security breaches. One way of dealing with this is through establishing minimum standards of security that contractors and other businesses that work with the government need to adhere to. The UK government has instituted a "cyber kite mark" security standard based on the ISO27001:2005 certification that businesses need to attain in order to bid for government contracts. In India, the National Cyber Security Strategy includes the encouragement of valid and certified IT products, and mandates secure application and software development that is based on global best practices.

d. Response – Regulation and Defence

In spite of having the best preventions in place, the vulnerability to cyber-attacks remain a reality. CERTs in particular are the frontline force with the capacity to react and defend networks and infrastructure against damage. In order to ensure a high capability for response, the various defence actors should be subject to regular drills, joint exercises and simulations that test their ability to respond to the latest global threats. Correspondingly, a legal platform should be established to empower the government and other actors to prosecute and seek redress from cyber security attacks. Regulation should ensure a balance between incentives and sanctions in order to adequately respond to and deal with attacks and threats when they happen.

e. Mitigation – Controlling the effects of a Security Breach

The economic and social impact that a successful cyber-attack could have is potentially devastating. In such an event, it is important that decisive measures are taken to restore confidence and re-build a secure infrastructure so as to mitigate the medium to long-term fall out of an attack. For example, an attack on a national airline carrier could erode public trust in the use of the airline for years which could severely cripple the industry. An effective crisis management and crisis communication strategy focused on rebuilding trust and giving assurance of redress measures is a critical component of this. Internally, governments should have established procedures for investigation, evaluation and consultation in order to identify and investigate systemic weaknesses and restore confidence. Feedback should be sought, both from the general public as well as partners to determine if the procedures in place are sufficient and improve the overall management of cyber threats and attacks.

Key Elements of a National Cybersecurity Policy

Structure	• Establish a Single National Body Responsible for Cybersecurity • Clearly Define Stakeholder Roles and Responsibilities • Establish a Functional, Timely Interagency Process
Strategy	• Issue a National Cybersecurity Strategy • Issue a Critical Infrastructure Cybersecurity Strategy • Maintain Up-to-Date National Cybersecurity Incident Response Plan for Critical Infrastructure • Craft Sector-Specific Plans as Appropriate
Stakeholder Engagement	• Establish Structure for Facilitating Public-Private Partnerships • Create Mechanism for Supporting National and Sub-National Governments
CYBERSECURITY AND THE GOVERNMENT	
Preparedness and Response	• Establish and Resource National Computer Emergency Response Team • Authorize and Encourage Timely Threat Information-Sharing • Ensure Calibrated Structure for Incident Reporting • Ensure a Consistent, Reasonable Standard for Personal Data Breach Notification • Establish a Transparent, Coordinated Process for Government Handling and Disclosure of Vulnerabilities
Government Procurement	• Keep Acquisition Technology Neutral • Ensure Use of Licensed Software • Ensure Software Is Vendor-Backed • Leverage the Security Benefits of Cloud Services • Build Security Considerations into Acquisition Processes • Manage IT Systems Smartly and Securely • Avoid Domestic Preference Requirements
Research and Development	• Support Research and Development of Cybersecurity Technologies and Tools
CYBERSECURITY AND THE PRIVATE SECTOR	
Critical Infrastructure	• Focus on Security Outcomes • Use Risk-Based, Flexible Policy Framework • Avoid Overbroad Definition of Critical (Information) Infrastructure • Align Critical Infrastructure Security with Internationally Recognized Standards • Ensure Any Certification Regimes Are Balanced, Transparent, and Internationally Based • Reject Requirements to Disclose Source Code and Other Intellectual Property
Consumer Products	• Promote Market-Driven Solutions • Ensure Any Certification Schemes Are Voluntary, Market-Driven, Broad-Based, and Internationally Aligned • Encourage Adoption of Internationally Recognized Standards
Data Flows	• Enable Cross-Border Data Flows for Business Purposes • Avoid Data Localization Requirements • Maintain a Policy Environment That Enables Emerging Technologies
CYBERSECURITY AND THE CITIZEN	

Awareness and Workforce Development	• Invest in Public Cybersecurity Awareness • Create Tools to Inform Consumer Choices • Build Cybersecurity Awareness into Every Level of Education • Prioritize Diversity in Cybersecurity Education and Training
INTERNATIONAL ENGAGEMENT	
Fostering International Cybersecurity Cooperation	Integrate Cybersecurity Cooperation into Foreign Policy Engage in International Cooperative Efforts Ensure Export Control Policies Do Not Impede Legitimate Cybersecurity Activity Prevent Territory from Being Used for International Cyber Attacks

Best practices

National Competent Authority for International Network and Information Security Coordination
Effective collaboration depends on clear, open lines of communication and agile coordination across a range of stakeholders. To facilitate such collaboration, a best practice is identifying a National Competent Authority (NCA) for network and information security, as directed in the European Union's 2016 Network and Information Security Directive. The NCA serves as the "single point of contact" to liaise with other governments in support of cross-border cooperation against transnational cybersecurity threats, and promote sharing of critical cybersecurity information across national stakeholders. The single national body assigned lead responsibility for cybersecurity will often serve as the NCA.

Convene Multi-Stakeholder Processes
The government can play an important role by convening targeted working groups, focused on a specific challenge or threat, that maximize the capabilities of the most relevant public and private sector stakeholders. Although private industry stakeholders are often willing to collaborate to address prominent current cybersecurity threats, such cooperation can be accelerated when a government is able to identify and convene relevant stakeholders, leveraging both its convening power and its intelligence-informed understanding of challenges and threats. Multi-stakeholder processes ensure that inputs from all relevant stakeholders in both government and private sector roles are addressed in the formation of a policy or operational initiative, and that stakeholders are invested in the outcomes.

NIST Framework for Improving Critical Infrastructure Cybersecurity
The United States National Institute for Standards and Technology (NIST) Framework for Improving Critical Infrastructure Cybersecurity is a voluntary, risk-based approach to managing cybersecurity risk that is intended to be applicable and scalable for organizations of all sizes and types, including critical infrastructure operators. It is structured around five core functions that reflect the full life cycle of cybersecurity risk management: identify, protect, detect, respond, and recover. These functions are further subdivided into 22 categories and 98 subcategories of guidance, which are mapped to internationally recognized standards (such as the ISO/IEC 27000 family of information security management systems standards) and other informative references. As such, the Framework:

- Is risk-based, flexible, and outcome-oriented
- Aligns with internationally recognized standards and risk management approaches
- Embraces public-private partnership
- Avoids dependency on indigenous technical standards
- Avoids burdensome regulatory schemes

The Framework is the baseline cybersecurity policy approach to strengthening cybersecurity across critical infrastructure. In fact, the US Government has directed that all federal government agencies, including the Defence Department and the Intelligence Community, use the Framework to guide their risk management programs. The Framework has been widely adopted by critical infrastructure operators, and it is expected that it will be adopted by more than 50 percent of all US organizations by 2020. Several other nations have begun to adopt substantively similar framework approaches, such as Italy's National Cyber Security Framework and Malaysia's MDEC Cybersecurity Industry Development Framework.

Avoid Overbroad Definition of Critical (Information) Infrastructure
Broad definitions cause uncertainty among business owners, their providers, and government agencies for compliance and during enforcement. Such definitions are likely to create costly regulatory burdens without actually improving cybersecurity, overwhelming infrastructure operators with obligations best reserved for those involved in supporting truly essential systems. Overly broad definitions can also lead to

overwhelming regulatory authorities with unnecessary information and oversight/ enforcement responsibilities. Instead, governments should adopt a definition of critical (information) infrastructure that focuses on truly essential systems, and apply a rigorous, proportionate, and risk-based analysis to determine what specifically should be designated critical (information) infrastructure.

Align Critical Infrastructure Security with Internationally Recognized Standards
Standards and best practices are most effective when developed in collaboration with the private sector, adopted on a voluntary basis, and recognized globally. Regulations, policies, and standards issued by a government to address critical infrastructure cybersecurity should be aligned with internationally recognized technical standards and internationally recognized approaches to risk management, such as the ISO/IEC 27000 and ISO/IEC 62443 series of information security management standards, the Common Criteria for Information Technology Security Evaluation, or the NIST Framework for Improving Critical Infrastructure Cybersecurity, as appropriate. Governments should particularly emphasize alignment with those standards developed through voluntary, consensus-based processes. Allowing critical infrastructure operators to combat evolving cybersecurity threats with evolving best practices and standards permits a more flexible, current, and risk-based approach to cybersecurity. Moreover, use of internationally recognized standards ensures interoperability for both businesses and government agencies with international counterparts, facilitating both economic development and operational collaboration against cybersecurity threats.

II. DATA PROTECTION

Information technology is in the process of transforming Myanmar's economy. With use of personal data driving many of the innovations being brought to market, issues such as individual consent, cross-border data flow and government access to data, have come to the fore. In framing a Data Protection Law, the government has the opportunity to provide a clear and consistent regulatory environment for data protection and data privacy. Data protection, including security, confidentiality, and preserving the integrity of data, is a core data management responsibility. A component of data protection is the protection of an individual's personally identifying information (PII), or privacy. We suggest government adopt a comprehensive, consistent, principles-based, risk-based data protection framework, underpinned by compliance with global standards and best practices. This approach will enable data-driven innovation and not be overly prescriptive, enabling growth of Myanmar's digital economy.

Key considerations when framing data protection law

a. Risk based approach

Government should create an environment that encourages participation and self-regulation to minimize risk and provide robust data protection. The data protection regime should incentivise development and use of privacy enhancing technologies and methods as a part of the risk-based accountability approach to data protection – that is, government data protection policy should encourage accountability to address risk of harm to individuals rather than establish a prescriptive set of compliance requirements. An example of a well thought out risk-based approach *for public policy* can be found in the APEC Privacy Framework, which recommends adherence to a set of privacy principles: Preventing Harm, Notice, Collection Limitations, Uses of Personal Information, Choice, Integrity of Personal Information, Security Safeguards, Access and Correction and Accountability. The Preventing Harm Principle recognizes a need to prevent misuse of personal information and consequent harm to individuals. Privacy protections, including self-regulatory efforts and education and awareness campaigns, should be designed to prevent harm to individuals from the wrongful collection and misuse of their personal information. Hence, remedies for privacy infringements should be designed to prevent harms resulting from the wrongful collection or misuse of personal information and should be proportionate to the likelihood and severity of any harm.

b. Principles-based Approach

Regulators must consider the privacy rights of a data subject (users) and abide by a set of principles intended to protect those rights. Listed below are data protection principles that regulators consider:

- **Fairness:** give accurate and full information about the purposes of processing, and any other information necessary to guarantee fair processing.
- **Lawful basis:** provide a lawful basis for data processing, i.e., deciding whether and for what purpose the personal data will be processed.
- **Purpose limitation:** personal data may only be collected for specified, explicit and legitimate purposes, and not further processed in a way incompatible with those purposes.
- **Rights of data subjects:** data subjects must be able to access their personal data, and obtain the rectification, erasure or blocking of personal data.

- **Accuracy:** ensure personal data is accurate and kept up to date.
- **Data security:** implement appropriate measures to protect personal data from accidental or unlawful destruction, accidental loss, alteration, unauthorised disclosure or access.
- **Data retention:** personal data should not be kept for longer than is necessary for the purposes for which it was collected or processed.
- **Transfer**: personal data should not be transferred to a country or territory unless the laws of country or territory, or the practices and contractual commitments of the transferee, ensure adequate protection of the personal data.

c. Consistency with International Standards and Best Practices

A Data Protection framework should leverage international industry standards and best practices. Corresponding third-party auditing provides assurance that effective physical and logical security controls are in place and avoids overly burdensome or redundant processes. The framework should be technology-neutral to ensure data protection and privacy rules can be applied regardless the technologies involved. Data governance is most agile and best conducted when it is technology neutral and structured around self-regulation based on international standards and best practices. There are many security frameworks, best practices, audit standards, and standardized controls that can be referenced, for example:

- Service Organization Controls (SOC) 1/Statement on Standards for Attestation Engagements (SSAE) International Standard on Assurance Engagements (ISAE) 3402 (formerly Statement on Auditing Standards [SAS] No. 70)
- SOC 2
- SOC 3
- International Organization for Standardization (ISO) 27001
- ISO 9001
- ISO 27017
- ISO 27018
- Federal Information Security Management Act (FISMA)
- Federal Risk and Authorization Management Program (FedRAMP)
- Department of Defense Risk Management Framework (DoD RMF, Cloud Security Model)
- Payment Card Industry Data Security Standard (PCI DSS)
- International Traffic in Arms Regulations (ITAR)
- Federal Information Processing Standard (FIPS) 140-2

Critical issues to be kept in mind

a. Data residency

Data residency requirements do not effectively serve the objectives of greater privacy protection and regulatory oversight and are harmful as they inhibit access to services of value to consumers and to industries. Countries that enact barriers to data flows make it harder and more expensive for their businesses to gain exposure and to benefit from the ideas, research, technologies, and best practices that accompany data flows and the innovative goods and services that rely on data. Restrictions on cross-border data flow also create trade barriers and impact business models. Studies show that data localization and other barriers to data flows impose significant costs: reducing U.S. GDP by 0.1-0.36%; causing prices for some cloud services in Brazil and the European Union to increase 10.5 to 54%; and reducing GDP by 0.7 to 1.7% in Brazil, China, the European Union, India, Indonesia, Korea, and Vietnam, which have all either proposed or enacted data localization policies.

In contrary, cross-border data flows can enhance data security in technologies such as cloud computing by allowing greater geographic diversity for data storage. Cross border data flows are essential to trade and gaining the greatest advantage of global economic opportunity. International flow of data contributed USD2.8 trillion to the global economy in 2014, a figure that could reach USD11 trillion by 2025. Over the past decade, data flows have increased world GDP by 10.1%. Thus, enabling cross-border data flows could result in a positive impact on an economy's GDP. This is supported by the evidence that efforts to reduce barriers to cross- border data traffic have been shown to drive growth.

b. Legal Access by Law Enforcement

Most countries have processes (including Mutual Legal Assistance Treaties or MLATs) to enable the transfer of information to other countries in response to appropriate legal requests for information (e.g.

relating to criminal acts). However, it is important to remember that each relevant law will contain criteria that must be satisfied in order for the relevant law enforcement body to make a valid request. For example, the government agency seeking access may need to show it has a valid reason for requiring a party to provide access to content, and may need to obtain a court order or warrant. For example, the Framework for the U.S.-India Cyber Relationship contains a commitment to sharing information on a real time or near real time basis, when practical and consistent with existing bilateral arrangements, about malicious cybersecurity threats, attacks and activities, and establishing appropriate mechanisms to improve such information sharing.

Best practices

Data Protection in Japan
In Japan, the Act on Protection of Personal Information (APPI) 2003 applies to both private and public sectors. In September 2016, Japan passed the "Amended Act on the Protection of Personal Information (APPI)" with implementing regulations released in January 2017. Japan's reformed privacy law came into full force May 30, 2017. Key changes under the new law include:

- Establishment of the Personal Information Protection Commission (PPC) which serves as the central supervisory authority for the APPI.
- The revised APPI provides specific guidance on the use of anonymized data (including approved methods for anonymizing data). This provision aims to enable and encourage use of big data analytics in Japan.
- Under the Amended APPI, exemptions have been modified in how the law addresses the transfer of Personal Data to an offshore entity. Specifically, when the counterparty is an offshore entity, the PI Business Operator will be required to either obtain the prior consent of the Subject, or confirm that such transfer of Personal Data will fall under an enumerated exception (the country in which the recipient is located (a) has a legal system that is deemed equivalent to the Japanese personal data protection system, or (b) is designated by the Japanese data protection authority; or the recipient undertakes adequate precautionary measures for the protection of Personal Data, as specified by the Japanese data protection authority).

Along with a significant number of changes, the new law also introduced a white-list concept, which will add Japan to EU's white list and make the EU, Japan's first "white listed" jurisdiction. The EU Commission has an existing white list of countries it has recognized in the past as having an adequate level of personal data protection to the EU. Importantly, Japan's participation in the APEC Cross-Border Privacy Rules scheme (APEC CBPRs), provides an exemption to cross-border rules in the Japanese legislation, where the receiving company is a certified APEC CBPR participant.

APEC Privacy Framework and Cross-Border Privacy Rules
The APEC Privacy Framework and Cross-Border Privacy Rules (CBPR) are a cross-region, principles-based approach which enables governments to develop national data protection laws that are appropriate for their particular circumstances, while ensuring uniform data protection goals are achieved. The APEC Privacy Framework and the CBPR, taken together are a framework for regional cooperation in enforcement of privacy and data protection laws among the 21 APEC member economies. Accountability is a key principle in the APEC Framework. Under the CBPR, accountability resides primarily with the business collecting the data to ensure that data is protected in compliance with the APEC principles. It provides for use of contracts and Binding Corporate Rules to transfer data to third parties or within conglomerates. Under the Rules, the person who collected the personal data is required to either obtain the consent of the data subject or to "exercise due diligence and take reasonable steps to ensure that the recipient person or organization will protect the information consistently with these Principles." The CBPR does not prohibit transfers to countries that do not have laws compliant with the CBPR. Rather, the CBPR requires the domestic entity transferring the data to another country, to be accountable to ensure the recipient of data protects the data in a manner consistent with the APEC privacy principles. Participation in CBPR is nascent but growing, with Singapore, South Korea, Japan, Canada, US, and Mexico participating, Australia and the Philippines committed to participate and many other APEC governments considering doing so.

III. E-COMMERCE

Myanmar is aiming to enact its first e-Commerce Law as part of its efforts to meet the goals set by the ASEAN Economic Community (AEC). Myanmar strengths lies in its competitive telecommunications sector, a growing tech-savvy youth population, innovative logistics solutions for the door-to-door delivery of e-commerce parcels and a fledgling tech start-up scene. To leverage these strengths, the country will require robust legislation to govern the rising volume of domestic and cross-border e-commerce transactions. However, the same legislation should avoid being overly prescriptive, considering the power of e-commerce to create jobs and increase trade in Myanmar. We commend the Ministry of Commerce and the government's commitment to making e-commerce a powerful engine for economic growth. However, this will require priority actions and adoption of industry best practices to accelerate the uptake of e-commerce and remove barriers to trade. In this regard, to fully realize the benefits of e-commerce, a national strategy that will align different stakeholders towards a common vision is an important step.

Given that e-commerce is important for the expansion of trade, inclusive growth and improved social conditions, most discussions in international forums focus on challenges in regulating different aspects of e-commerce and ensuring that regulations do not act as barriers to the growth of this sector and trade. Unless the sector is regulated, it can lead to several issues such as violation of e- contracts, tax evasion, violation of privacy, piracy, spam, lack of consumer protection for online purchases, and sale of restricted products online. While consumers and businesses can get cheated and legitimate businesses can face loss of revenue, governments can face loss of income through tax evasion. Hence, it is necessary to regulate this sector, and both developed and developing countries acknowledge it. Some of the key elements of the regulations involved in this sector include privacy policy, anti-spam laws, compliance of payment cards with data security standards, consumer protection regulation for non-store purchases, e-contract regulations, regulations governing IT, and new technologies such as cloud computing, anti-competitive regulations, trademark, patent copyright regulations, and regulations related to financial transactions and taxation. At the same time, it is also important to ensure that regulations are not unnecessary barriers to trade and growth of the e- commerce sector, and they should support the development of technology and business models. Given the fast-paced growth of the sector globally, it is necessary for a country's regulations to protect the sector, promote growth and create an enabling environment for businesses.

This promise also presents highly attractive growth opportunities to create a cashless society, which will help restrict the shadow economy, increase tax revenues and curtail criminal activity by making it increasingly difficult to hold wealth outside the formal economic system. For instance, the Reserve Bank of Australia (RBA) is aiming to make Australia a largely cashless society by 2020, relying heavily on the use of mobile platforms for digital commerce activities. The New Payments Platform (NPP) supported by the RBA and 12 founding financial institutions, enables cheap, secure, 24/7/365 instantaneous payments. It works by establishing a PayID – which could be a mobile phone number, email address, or business registration number – and linking that to the user's bank account so that payments can be made through existing online and mobile banking apps, or other new apps that will take advantage of the platform.

Multilateral trade agreements can further accelerate the development of such initiatives by facilitating interoperability between national systems and aligning, or harmonising, regulatory requirements. The benefits that stand to emerge from interoperability across data flows, financial transactions, identity and commerce, have been recognised in the recently concluded Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP).

E-commerce, which invariably involves cross-border data flows, has the potential to expand opportunity and foster equal access to the benefits of technologies such as cloud computing because it brings global marketplace to every consumer with an internet connection, while enabling even the smallest local business to reach consumers and suppliers anywhere in the world. To ensure that e-commerce reaches its full potential, any regulatory framework accompanying e-commerce should refrain from imposing custom duties or other taxes on cross-border electronic transmissions and commit to extending nondiscriminatory treatment to digital products and services.

Countries Changing and Implementing E-commerce Regulations

- **AUSTRALIA:** Australia amended its Electronic Transactions Act 1999 in June 2011 to make electronic transaction facilitation easier, promote business and community confidence in the use of

electronic transactions, and enable business and the community to use electronic communications in their dealings with government.

- **HONG KONG:** Hong Kong enacted the Electronic Transactions Ordinance in 2000 (updated in 2004) to facilitate the use of electronic transactions for commercial and other purposes, to provide for matters arising from and related to such use, and to make connections via technology easier. Moreover, there is no requirement under the Hong Kong law for a company to first set up a presence in Hong Kong for its online business before its services and products can be provided to people or businesses in Hong Kong.
- **SINGAPORE**: As Singapore prepares to transform itself into a global e-commerce hub in the face of strong global competition, an array of initiatives and grants have been rolled out by various government agencies in support of e-commerce investments.

- *Retail Industry Transformation Map (ITM*): The 2020 vision of the Retail ITM is for Singapore to have a vibrant retail industry. This comprises a mix of highly productive omni-channel retailers and local brand owners with global footprints, all supported by a professional and skilled workforce. With the Retail ITM, retailers can look to strengthen their enterprise capabilities to increase their productivity, and make their presence felt in the global arena with a more vibrant sector supported by a skilled workforce.
- *Economic Development Board's (EDB) Industry 21 blueprint*: The Info-communications Media Development Authority (IMDA) teamed up with EDB and the industry to define and adopt common IT standards to enhance seamless B2B documents exchange among companies for the electronic cluster. The plan to accelerate the use of e-commerce comprises of five main thrusts, namely to develop an internationally linked e-commerce infrastructure, jump-start Singapore as an e-commerce hub, encourage its strategic usage by businesses, promote its usage by the public, and to harmonise cross border e-commerce laws and policies.
- *Start-ups community*: For start-ups looking to enter the e-commerce landscape, the Action Community for Entrepreneurship (ACE) is a support platform designed to provide a holistic package to further nurture a vibrant and connected start-up ecosystem. E-commerce start-ups are also able to tap on the various support schemes provided by ACE ranging from corporate innovation to peer group mentoring as well as access to international markets and communities championing the global startup scene.
- *Networked Trade Platform (NTP):* The Inland Revenue Authority of Singapore (IRAS) has also rolled out its plans to support e-commerce investments in Singapore. The Networked Trade Platform (NTP) is an advanced trade information management platform to support companies in the trade and logistics industry and adjacent sectors such as trade finance, where importers and exporters would have access to all government-related and commercial trade services. This mainly involves the electronic bill of landing and sea freight e-commerce. The NTP will help businesses boost productivity by streamlining work processes, reducing inefficiencies of manual trade document exchange, and leveraging data analytics for insights from their trade data, so as to be well-equipped for the digital economy. It also enhances the competitiveness of local SMEs in the field of e-commerce with regards to international trade and promotes Singapore as a strategic destination of choice for traders, shippers, logistics and trade finance companies around the globe.

End of submission