美中贸易全国委员会关于《中华人民共和国网络安全法（草案二次审议稿）》的修改意见

2016 年 8 月 4 日

美中贸易全国委员会谨代表近 200 家会员公司非常感谢能够有机会就全国人民代表大会最新的《中华人民共和国网络安全法（草案二次审议稿）》提出修改意见。我们的会员公司广泛地分布于各行各业，其中既包括购买和提供信息安全产品和服务的公司，也包括经营和使用信息网络的公司。虽然这些会员公司不尽相同，但他们都秉承同一信念：促进并参与支持中国的开放和健康的商业环境建设，推动信息技术的应用作为经济增长的驱动力。

美中贸易全国委员会及我会员公司认识到《网络安全法（草案二次审议稿）》体现了中国政府力求促进信息安全、保障中国公民和组织机构的合法权益的愿望。我们的会员公司持有同样的目标，并且在全球范围内拥有与政府以及业界同行合作的丰富经验。这些经验能够帮助实现上述目标，同时促进行业的切实发展。我们很多会员公司长期在中国提供高质量的信息安全产品和服务，为这个行业的发展做出了积极的贡献。

我们欢迎草案倡导在网络空间治理中更好地进行国际合作、发展技术和网络空间标准，努力应对违法犯罪活动。草案鼓励以行业为主导制定网络安全标准，修订了个人身份信息的定义以排除 IP 地址，对此我们也表示欢迎与赞许。

若本草案能阐明并确保一审稿（一审稿草案说明第二章）中首次提出的同等对待国内外企业，那将是非常有益的。我们也鼓励中国在实施本法时充分借鉴国际标准和行业最佳实践，不过度规定、损害国际商务活动。

我们鼓励全国人民代表大会在进一步修订这部法律草案的过程中确保政府流程的透明和这部法律与中国其他法律法规的一致性，以及各部门执法口径的统一性。此外，在起草这项法律以及其他相关文件时，如第四条中提到的网络安全战略，我们鼓励全国人民代表大会同相关行业中包括外资企业在内的各从业公司积极交流。行业高度关注的问题如下，包括：

- 强制性标准和已由公司制定、国际上使用的现有标准之间的关联（第十条）；
- 术语“安全可信”的使用（第十五条）；
- 发展网络安全等级保护制度的定义（第二十条）；
- 留存网络日志的要求（第二十条）；
- 报告网络事件的适用范围（第二十四条）；
- 关键信息基础设施（第二十九条）和网络运营者（第七十二条）的定义及适用范围；
- 认证、检测流程以及网络关键设备及相关产品的适用范围（第二十二条、第三十三条和第七十二条）；
- 数据本地化和跨境信息自由传输的相关问题（第三十五条）。

我们注意到《网络安全法》是新近更广法律框架中的一部分，其他还包括起草中的网络安全战略、《反恐怖主义法》和《国家安全法》。美中贸易全国委员会鼓励阐明本草案将如何与这些措施和现有的法

律、法规相互作用，包括但不限于中国的《刑事法》、中国网络安全审查制度的制定以及现有的、中华人民共和国公安部 2007 年颁布的多等级保护制度框架。

美中贸易全国委员会非常高兴能够对草案提出意见。我们建议对草案中的一些条款，以及对附加给公司和政府部门实际上可能阻碍实现《网络安全法》目标的义务做进一步的阐明。综合地解决这些问题可以鼓励公司为中国带来其最好、最安全的技术，从而确保中国的信息安全。

定义及适用范围

第二条为该法描述了一个宽泛的适用范围，规定其适用于在中华人民共和国境内网络的建设、运营、维护和使用。随后的条款从不同方面明确了法律的适用范围， 例如网络运营者、关键信息基础设施以及公民个人信息。虽然第七十二条对该法案的一些关键词给出了定义， 但一些定义仍存在一些问题：

- **关键信息基础设施：**第二十九条规定对“关键信息基础设施”将实行重点保护，且关键信息基础设施的具体适用范围将由国务院制定。因没有定义该术语且该术语基于宽泛的概念，如国家安全、经济、民生和公共利益，该条款涉及的行业范围将包括大量可能实际并不是关键的信息系统。

  美中贸易全国委员会建议监管部门清晰、狭义地界定关键信息基础设施的适用范围，使其仅包括核心功能所必需的、特定的基础设施。若不缩小适用范围，关键信息基础设施可包括信息通信技术行业的所有功能，这将给公司合规和政府部门执法带来挑战。定位有范围的执法和合规资源将促进实现中国的网络安全目标。

  我们鼓励监管部门与公司、行业协会、国际组织和其他利益相关者共同协作，阐明关键信息基础设施的定义。我们建议国务院发布定义草案，向社会征求意见后再确定，并延迟实施《网络安全法》，直至阐明、发布这些界定概念。我们也建议对“关键信息基础设施运营者”提供额外的定义，并进一步阐明这一定义与其他法律法规中的相关术语如何相互区别或统一，例如《公共安全法》中述及的“关键基础设施”。

- **安全可信：**第十五条提倡使用“安全可信”的网络服务和产品，但并未界定该术语。由于其与“安全可控”一词近似，且后者已经引起外资利益相关者的担忧，美中贸易全国委员会建议监管部门与该行业国内外企业合作，清晰定义这一术语，制定客观、透明、公平及有技术基础的标准。我们进一步建议定义术语时应反映双边承诺，即技术安全与产品国籍无关，而是与安全性能和流程的技术评估有关。

  美中贸易全国委员会了解中华人民共和国国家互联网信息办公室下属的全国信息安全标准化技术委员会正在制定安全可控技术的相关标准。我们鼓励监管部门继续与外资公司及利益相关者协作，采用国际最佳实践和安全标准来制定标准，以保证中国国内网络环境的健康发展。

- **网络安全等级保护制度：**第二十条规定中国将采用网络安全等级保护制度，包括保障网络免受干扰或者未经授权的访问，防止网络信息泄露或者被窃取的义务。草案并未明确这一等级体系与现有制度的关联，例如涉及技术相关产品在中国如何认证销售的、2007 年颁布的多等级保护制度。美中贸易全国委员会提请监管部门阐明本草案中的网络安全等级保护制度将如何与现有的多等级保护制度相互关联——例如它将如何对现有的多等级保护制度框架进行升级、补充、替代或整合。

  中国现有的多等级保护制度框架曾引起了外资公司的担忧，因其歧视性条款规定在当地注册知识产权，移交敏感源代码。若《网络安全法》草案下的网络安全等级保护制度将与现有的多等级保护制度框架进行整合，我委员会鼓励监管部门去除歧视性语言，即禁止使用数据处理级别为“第三级”及以上级别的外国产品。

我们建议中国整合多等级保护制度，提高明确性，减少监管负担，确保同等对待外资企业与国内企业。我们也建议国务院在该领域采取的措施应与其他的政府安全举措保持一致。

- **网络运营者**：第七十二条第（三）款定义网络运营者为“网络的所有者、管理者以及网络服务提供者。”美中贸易全国委员会欣赏这项定义界定的范围较法案一审稿已经进行了简化，但我们担心该定义仍过于宽泛，几乎包括了所有使用电信或互联网服务的公司。例如公司运营一个非商业性的网站，提供公司信息或是推广线下业务。与他们的网络运营者相比，这样的网站安全风险较小。将网络运营者的一切责任施加于这些公司之上会极大地增加公司的运营成本和许可困难，并最终限制他们通过网络为其客户提供服务的能力。

除此之外，目前法律的表述可以将这些责任同样适用于公司内部的网络，公司可能因此会被要求在他们的官方网络上监视员工的个人行为，这会导致个人隐私问题。

我们建议明确 “网络运营者”的定义，细化在中国境内建设、运营、维护网络的电信、互联网、网络硬件及网络软件提供者，并将适用范围缩小至提供给终端客户使用的公共网络。这可以将非商业性网站和网络（包括公司内部网络）排除在外。此外，我们还建议参考其他相关法规，如《互联网信息服务管理办法》，修改定义，以保持一致性。

- **强制性网络安全标准**：第十条规定了强制性国家标准的合规要求。强制性网络安全标准不应要求公开源代码，使用当地的加密标准，或任何可能影响知识产权使用和保护的其他负担。美中贸易全国委员会建议应更多考虑全球自愿标准和最佳实践，这些都是经过多年的测试并参考了国际专家发展形成的。这些要求不应限制外国公司采用其现有的全球安全措施为他们在中国的用户、网络、业务和客户谋利。

- **“公民个人信息”、“重要业务数据”和跨境安全审查**：第三十五条规定关键信息基础设施运营者必须保存在中国大陆范围内的公民的个人信息和“重要业务数据” 并规定这些数据必须在经过安全审查后方可离开中国。

第七十二条第（五）款对个人数据的定义宽泛，相关条款规定其包括“识别公民个人身份的各种信息。”我们建议阐明该定义，让公司确保合规。美中贸易全国委员会也建议阐明本草案涉及的个人数据的条款如何与其他法律法规中其他类似条款相互关联，例如《消费者权益法》、《刑法》修正案（九）以及 2015 年国家工商行政管理总局颁布的《侵犯消费者权益行为处罚办法》中的隐私条款。

草案也未定义“重要业务数据”的适用范围。为了让公司能够遵守这些条款。美中贸易全国委员会建议监管部门排除商业或经济方面的考虑，严格按照国家安全的相关考虑阐明并狭义定义“重要业务数据”。

美中贸易全国委员会还建议监管部门阐明数据流动的安全审查将如何与现有的管理海外数据传输的规定相互联动，并提供相关的细化规定、验证或认证程序细节，或取得资质必须完成的其他程序的详细信息。为了确保与全球最佳实践相一致、中国与全球数字经济的顺利整合，我们建议延迟实施本法，直到公布这些细节供国内外的利益相关者提供意见和建议。

- **其他事项**：一些术语——例如第三条中的“积极利用”；第十一条中的“网络相关行业组织”；第十四条中的“网络产品、运行和服务”；术语“用户”在草案中可以指政府、企业实体亦或是个人；第二十四条中的“网络安全事件”；以及第四十六条中的“电子信息发送者和应用软件提供者”、“电子信息发送服务提供者”和“应用软件下载服务提供者”。我们建议根据与国内外利益相关者咨询的结果对这些术语进行明确定义。

信息安全产品认证

第二十二条指出网络“关键”设备和网络安全“专用”产品在中国境内销售前，需根据特定产品目录，通过安全检测和认证程序。第三十三条进一步指出当关键信息基础设施运营者采购此类产品时，产品需通过附加的安全检测。但以上条款均未明确安全检测的流程细节或上述两条款如何联动。

这引起了网络科技相关公司的几点担忧。首先，两项检测认证的流程存在一些重要的疑问，尤其是公司是否会被要求披露源代码或采用当地的加密算法。尽管草案没有明确说明认证流程，但近期的其他政策已经引发类似的担忧，例如银监会发布的《银行业应用安全可控信息技术推进指南（2014-2015 年度）》，这些要求让公司的核心知识产权面临潜在危险，可能危及他们的竞争力和创新能力。此外，在第十条已经要求这些产品和服务应当符合相关的国家标准和行业标准的情况下，此类认证流程是多余的。

其次，第三十三条要求采购者在购买网络产品和服务时需通过安全审查，对此企业和政府有关部门都是备受挑战。采购公司从技术公司处购买产品或服务时，通常情况下无法取得源代码和产品的知识产权，这将给遵守第三十三条造成困难。在诸如金融服务等行业，国际市场上的合规规定也不允许做此类披露。这个领域的中外企业都将无法在不违反国际规则的情况下遵守此草案中的要求。

第三，条款没有明确何谓“关键”和“专用”，鉴于草案中没有说明何种产品将被列入目录， 这给那些需要确定其产品是否适用于条款的公司带来了不确定性。

公司现已将其产品处于严格的安全测试和认证流程之下，其测试与认证均基于全球市场的国际要求和标准。要求公司接受国家层面的安全审查，并依据外资公司可能无法满足的标准选择硬件、软件或服务，将阻碍中国国内公司使用最好的产品，进而限制其网络的安全。

此外，强制公司从预先批准的、中国特有的技术设备和解决方案中作出选择，而不是让他们利用其已在全球网络中采用的技术，可能会破坏或削弱中国境内公司的安全操作。例如，如果中国孤立的本土网络发生数据泄露或被盗，全球监控系统因网络不兼容而不能迅速发现，则可能会严重影响公司的响应速度、遏制数据泄漏的能力以及提醒客户的及时性。这样的后果不利于中国提高信息技术安全的总体目标。

我们建议删除第二十二条和第三十三条，或修改相应条款以针对条款中提及的产品范围和检测认证过程进行更加详细的说明。如要修改这些条款，我们还建议修改后条款明确说明允许符合资质的私营机构，包括外资机构进行符合规范的安全检测认证，并且政府和私营机构应该努力确保认证检测标准和流程的统一执行。

跨境网络数据传输

第三十五条要求关键信息基础设施的运营者应当在中华人民共和国境内存储其在运营中收集和产生的公民个人信息等重要数据，且仅在经过安全评估后方才可在境外存储或者向境外的组织或者个人提供。这种对境内数据本地化储存和转移的要求，会将中国公司孤立在最好的数据相关技术和业务专长之外，阻碍中国在信息技术领域的发展。此类限制将不仅阻止中国与全球信息通讯技术生态系统的深入一体化，并有可能给中国政府诸如发展云技术和智能技术服务等政策目标带来不利影响。

数据本地化的要求可能会增加在中国运营的公司的成本和监管困难，而不会提高数据的安全性。由于数据存储和检索技术的发展，限制数据存储的物理位置并不会降低在中国境外泄露数据的风险，反而确实限制了外资公司采用全球统一的信息技术安全系统的能力。统一的系统对确保日常全球运营能力意义重大，也是全球监测网络识别安全漏洞、数据泄露、窃取或其他违法犯罪及有危害的活动中必不可少的一部分。数据本地化要求公司使用当地的信息技术解决方案，而这些方案可能不会立即或完全与公司的全球网

络安全框架兼容。使用与全球安全网络不同步的解决方案会导致安全隐患，尤其是已在中国收集的数据，从而与本草案信息安全的目标背道而驰。

限制跨境数据传输更令人担忧。此类数据传输对助推信息产业以及经济的总体发展的全球数字经济的发展至关重要。数据向海外传输前的强制性安全审查可能会制约安全流程，从而对安全性造成负面影响。例如，当一个中国顾客在中国的银行的国际支行办理业务时自愿提供个人信息以验证交易；或当一个中国公民与境外亲友交换信息；这些情况尽管都经当事人同意，却还是可能会被认定为在条款范围之中，并被要求经过安全评估。限制数据流动的条款也会带来其他问题，包括关键信息基础设施运营者的定义、条款所覆盖的数据的类型（如商业专有信息或人力资源数据）、申请安全评估豁免的细节以及要求评估的范围（例如，是否只适用于新收集的数据，还是只适用于现存数据）。

美中贸易全国委员会强烈建议与该行业利益相关者商榷后修改第三十五条，以保证规范网络数据流通的尝试能够充分考虑网络安全和实际商业需求。对此问题的开放讨论将更好地确保中国维护本国网络安全，同时促进其信息通讯技术部门领域的可持续发展。

网络安全标准

美中贸易全国委员会赞许第十四条中关于鼓励企业参与网络安全国家标准和行业标准制定的特定内容。与业界间积极，开放的互动是确保标准能够全面，可实现，并 被广泛接受的最佳途径。技术安全标准草案应反映双边承诺，即技术安全与产品国籍无关，而是与安全功能和流程的技术评估有关。我们希望中国政府确保标准制定的透明度，同时建议能够在第十四条中添加条款明确“本国、合资和外资企业均有资格参与标准制定”。

此外，我们强烈建议草案中的表述能尽可能地与国际标准和最佳实践保持一致。与国际标准更大程度上的一致性将会满足中国消费者的需求，为他们的网络安全保护提供最多的选择；同时也能够满足中国公司的需求，使其能够更容易进入全球市场。反言之，中国特有的标准体系会由于减慢该行业对于升级的网络威胁的反应速度，妨碍此草案的目标。我们建议在草案中的相应条款增加这方面的表述，如第十、十四、二十一以及二十二条。

网络运营者的责任与义务

本草案涉及网络运营者的义务及其未能遵守该法律规定时所需承担的法律责任。

- **第二十条第（三）款**要求网络运营者应留存网络日志不少于六个月。“网络日志”的适用范围非常宽泛，其内容可以是记录登录网络或设备的使用者，也可以是基于访问控制列表，记录允许或拒绝哪些连接，亦可以是记录每部分的每个数据包。为减轻合规的操作负担，美中贸易全国委员会建议本草案表述应阐明公司必须保留“与安全事件直接相关的网络日志。”

- **第二十一条**要求网络产品、服务应当符合相关标准，并要求企业在收集用户信息或发现存在安全风险时及时告知用户。该条款同时要求网络运营者在合同期内为其产品、服务提供安全维护，却未明确在合约提前中止或对方违约的情况下，企业是否仍有此义务。此外，该条款存在诸多问题尚未阐明，包括企业应当如何征得用户同意，以及在第三方修改产品或错误安装产品的情形下，企业是否仍需承担责任。我们建议对该条款增加新内容，以解决上述疑虑。

- **第二十一、二十四、四十一、五十三和五十八条**都要求网络运营者在发现安全风险或网络入侵时“及时”采取补救措施，告知用户，并向有关主管部门提供信息，然而法案尚未明确界定“及时”。鉴于第六章规定了当企业未能遵照上述规定时所应承担的法律责任，此处的定义不明使我们非常担忧。存在安全风险时，企业往往在告知用户之前就采取补救措施，防止可利用漏洞的消息扩

散，之后再保护合法用户。我们建议将“及时”改为“运营者发现安全威胁后在切实可行范围内尽快”。

- **第二十一条和四十六条**禁止网络产品、服务提供者或应用软件提供者安装设置恶意程序。这两条都容易引发疑问，即当第三方或恶意员工在公司不知情的情况下安装这类软件时，公司是否应该承担责任。我们建议向两条中添加新表述，规定“软件应用提供者不得*故意*分销包含恶意程序的软件”，或者规定软件应用提供者应采取合理的预防措施，防止分销含有恶意程序的软件。

- **第二十三条**规定提供重要服务的网络运营者要求用户提供真实身份信息，并且禁止其为不提供相关信息的用户提供相关服务。这样的要求可能与中国保护用户隐私和安全的目标相冲突，并且同时也向网络运营者提出了严峻挑战。此外，这些要求对企业来说执行过于繁重，尤其是在服务提供者不知晓用户向其伪造身份的情况下。

这些规定使网络攻击者可掌握的公民个人资料缓存量增加，进而导致个体网络事件，增加个体网络事件带来的风险。因此，我们希望全国人大按照国际最佳实践与利益相关者共同修订这些规定。美中贸易全国委员会也建议监管部门明确除了“信息发布”和“即时通讯”服务之外，哪些类型的服务需要实名身份验证。

- **第二十五条**规定，当网络运营者进行认证或评估，并发现漏洞时应当遵守国家有关规定。标准的做法是，这些漏洞将作为认证或评估的一部分被修正。美中贸易全国委员会建议草案进一步阐明“有关规定”，提供适用于第二十五条规定的具体例子。

- **第二十七条和四十七条**允许政府机关在进行安全和刑事调查时要求网络运营者提供技术支持和协助，但是条款没有进一步细化企业可以或应当提供协助的范围。美中贸易全国委员会建议明确定义网络运营者在这些情况下的责任，其应包括网络运营者在这些情况下要提供的活动、信息或文档。

- 同样的，**第三十二和三十六条**也应该修改增加新的表述，要求政府尽量减少检测评估对网络运行带来的负面影响，要求承担职责的有关部门保护专有信息、商业秘密以及知识产权，并要求这些检查行为接受政府监督。我们还建议增加与修改后的第三十二、三十六和四十三条一致的新表述，即要求任何疏于保护商业秘密、保密信息或公民个人信息的政府官员对其行为负责。

- **第三十四条**要求关键信息基础设施的运营者与设备提供者签订协议，明确安全和保密义务与责任。然而，此类协议的范围并没有明确，使网络运营者与设备提供者均难以确保符合规定。我们建议中国政府公布此类协议的更多细节或提供此类协议的模板。

- **第三十九至四十八条**讨论了网络运营者的隐私义务包括他们应当如何处理个人信息、保护隐私及应对实际或潜在的信息泄露。这些条款被视为总体原则。美中贸易全国委员会建议增加表述，阐明网络运营者或其他处理个人数据的经营体的义务以及适用的隐私条款。此外，我们鼓励中国参考国际最佳实践，包括《APEC 隐私保护框架》，作为创建正式数据保护机制的有效基础。

第四十三条禁止非法销售个人信息。我们建议本条款界定“合法”透露给第三方和“非法”披露信息之间的差异。更明确的说明将确保公司正确了解如何在这些条款要求下如何处理一些重要业务，例如消费者分析、网络广告或通过分析个人信息为特定的消费群体提供定制服务和产品。

- **第四十五条以及第四十八条**要求网络运营者在特定状况下停止传输用户发布的信息。这里有两个问题：1）运营者停止传输信息的能力通常取决于用户发布信息的具体方式。例如，普通网站上和社交媒体平台上的信息传输是完全不同的。我们鼓励全国人大直接与网络运营者密切合作，修改第四十五条以确保网络运营者在合理的标准内处理这些信息；2）除非网络运营者受到保护，否

则政府对停止信息传输的要求有可能使其承担来自被影响用户追究的法律责任。对此，我们建议在第四十五条中增加保护网络运营者不受这类法律责任影响的新的表述。

- **第五十一条**倡导建立网络安全风险评估和应急工作机制，以制定适应不同行业和领域的网络安全应急响应方案。美中贸易全国委员会建议国家级网络空间管理官员与国内外业界携手合作，充分利用他们的商业视角和专业技术知识。美中贸易全国委员会建议建立一个共同的框架以确保各领域之间的一致性，这将缓解开展跨行业业务的公司在落实这些方案时的压力。

- **第五十六条**允许政府部门对网络通信采取限制等临时措施，目的是在“重大突发社会安全事件”中维护国家安全和社会公共秩序。但是，该条款并未解释这类事件的具体内容，也未明确具体可以采取的措施及持续时间。这些有待明确的部分让可能行使这些权力的政府部门存疑，也让需要了解这些限制对自身运行影响的网络运营者。我们建议增加新的表述，定义可采取措施的范围和种类、允许的持续时间，以及要求政府在采取这些措施时提出相应的法律依据。

网络漏洞检测

第二十六条和三十六条在网络漏洞检测的问题上包含了矛盾的内容。第三十六条规定关键信息基础设施的运营者应当自行或者委托专业机构，对其网络的安全性每年至少进行一次检测评估。该条款内容意味着允许企业雇佣外部专家通过漏洞扫描和内部安全入侵检测等手段进行系统评估。然而，由于第二十六条禁止任何形式的网络入侵，继而限制了企业从事第三十六条所提倡的用以增强网络安全的行为。这一矛盾有可能导致企业判定即便是得到授权的漏洞扫描都是被禁止的，从而限制了他们确保自身网络安全的能力——进一步阻碍实现本法律的总体目标。

我们建议对第二十六条进行修改，规定“任何个人和组织不得从事入侵他人网络、干扰他人网络正常功能、窃取网络数据等危害网络安全的活动，除非受到网络运营者授权作为其安全测评的一部分；不得提供从事入侵网络、干扰网络正常功能、窃取网络数据等危害网络安全活动的工具和制作方法；不得为他人实施危害网络安全的活动，例如故意提供技术支持、广告推广、支付结算等帮助。”这样具有针对性的内容，可以保留原条款防止网络犯罪行为的本质，同时也给予企业常规检测其网络漏洞的自由。

结论

美中贸易全国委员会非常感谢全国人民代表大会给予我们机会就**《中华人民共和国网络安全法（草案二次审议稿）》**提出意见。我们希望这些意见在全国人民代表大会法律委员会审核本法的工作中起到建设性和有效的作用，同时我们期待有机会继续讨论以上意见内容。

—完—

美中贸易全国委员会
联系人: 彭捷宁 Jacob Parker，中国区副会长
电话：010-6592-0727
传真：010-6512-5854
邮箱：jparker@uschina.org.cn