美中贸易全国委员会对《中华人民共和国数据安全法（草案）》的意见

2020 年 8 月 14 日

美中贸易全国委员会（USCBC）代表 220 多家会员企业，感谢有机会向全国人民代表大会提交对《中华人民共和国数据安全法》草案（以下简称草案）的反馈意见。

我委员会收到了来自信息和通信技术、汽车、服务和金融等行业企业对该草案的意见。

该草案涉及一项重要而复杂的议题——当今世界许多国家的政府都在讨论，如何既能确保数据保护系统的完整性、又不给行业带来过度或不必要的负担，实现最优监管。我们尤其强调以下建议：

范围以及与其他法律的关系：草案的范围过于宽泛，涵盖了电子或非电子形式的任何数据，这给企业带来了潜在的合规负担。此外，现有的一些法律、法规和标准已经涵盖了草案中涉及的一些国家安全要素。这包括《网络安全法》、《民法典》、《国家安全法》、《数据安全管理办法（征求意见稿）》和《个人信息出境安全评估办法（草案）》。我们希望全国人大确保上述法律法规之间的监管一致性，并避免现有法律法规与本草案的重叠。

重要数据：我们认为，可以通过定义“重要数据”和“重要数据的处理者”增加清晰度，同时限制重要数据风险评估的范围和必要性，以进一步改善草案。根据现有法律法规，重要数据应本地化并接受跨境安全审查。因此，我们建议草案的定义与《数据安全管理办法（征求意见稿）》保持一致，按照后者规定，大多数公司数据不包括在重要数据的范围内。此外，草案要求“各地区、各部门”创建自己的单独目录，增加了不同省市制定不同目录和合规要求的风险，这可能会妨碍企业日常运营所需的数据自由流动。因此，我们建议统一“重要数据”的定义权限。

数据分类和等级保护 2.0（MLPS 2.0）：草案第 19 条规定，数据将根据其对中国国家安全的重要性进行分级和分类。我们建议将这一分类系统与现行等级保护 2.0（MLPS2.0）保持一致，避免公司要遵守多个不同的国家安全合规制度。

个人信息和数据：草案对数据的定义宽泛，不清楚是否包含个人信息。根据《网络安全法》，个人信息和重要数据是两个独立的概念，到目前为止，这两个概念由不同的标准和法规分别管理。在草案的数据定义中包含个人信息将违反现有法规，让公司不易理解合规要求。我们建议草案明确将个人信息排除在数据定义之外，以确保与现行法律保持一致。

治外法权：第二条规定，中国境外的组织和个人开展数据活动，损害中国国家安全利益的，适用本草案。目前还不清楚将利用什么机制来执行这一规定，也不清楚哪些数据活动被认为有损中国国家安全。这加剧了对中国数据和网络法规中基于国家安全的法规和审查日益增多的担忧。此外，企业指出，有更适当的法律如《国家安全法》，来解决第二条所述的问题。因此，我们建议删除这一条款。

监督：负责监督和执行该草案的政府部门不明确，在某些情况下可能存在监管重叠，会导致混乱。为了避免重复监督，不同的政府部门应明确指定各自的执法和监督单位。

跨境数据流动：跨境数据流对跨国公司与总部进行沟通以及开展日常业务(如“了解客户”和“反洗钱”活动)非常重要。全球数据的自由流动和交换，是创新和全球经济的重要支撑。我们高兴看到，草案第十条承诺促进数据自由流动。我们的会员企业希望具体了解跨境数据安全与跨境数据自由流动如何实现平衡。

美中贸易全国委员会感谢有机会提出意见，并在后文提供了针对具体条款的详细建议。

意见与建议列表			
章节	条款内容	意见	建议
第一章	总则		
2	在中华人民共和国境内开展数据活动，适用本法。 中华人民共和国境外的组织、个人开展数据活动,损害中华人民共和国国家安全、公共利益或者公民、组织合法权益的,依法追究法律责任。	1) 第二条第一句规定，在中国境内开展数据活动，适用本法。第二段第一句却提及中国境外开展的活动。 2) 该条境外要素的适用条件模糊、宽泛。 3) 不清楚有关部门如何对不在中国境内的组织、个人执法。 4) 本条未定义损害中国国家安全、公共利益或者公民、组织合法权益的数据活动。该规定过于宽泛，难以确立对合规的基本理解。	我们建议 1)删除本条第二段，只关注中国境内的数据活动。 2)对于中国国家安全面临的海外威胁，我们建议依据现行法律法规，如《国家安全法》和《民法典》，以避免不必要的重叠和重复。
3	本法所称数据,是指任何以电子或者非电子形式对信息的记录。 数据活动,是指数据的收集、存储、加工、使用、提供、交易、公开等行为。 数据安全,是指通过采取必要措施,保障数据得到有效保护和合法利用,并持续处于安全状态的能力。	“数据”、“数据安全”和“数据活动”的定义宽泛、模糊，可以涵盖商业活动的所有方面。《网络安全法》对个人信息和重要数据进行了区分。然而，第三条似乎没有包含这一区别，导致草案与《网络安全法》和建议的《个人信息保护法》出现不一致。 “提供”数据的范围不应包括向关联公司、子公司或股东提供的数据，无论他们是否在中国境内。	我们建议草案应缩小定义的范围，澄清“数据”、“数据活动”、“数据安全”、“处理”、“交易”等关键概念的定义，以确保相关法律法规中这些术语的定义一致。公司努力确保在数据的整个生命周期中对其进行保护，如果没有这样的澄清，将对公司合规造成重大挑战。

6	中央国家安全领导机构负责数据安全工作的决策和统筹协调,研究制定、指导实施国家数据安全战略和有关重大方针政策。	目前还不清楚这些条款中提到的是哪些政府机构，特别是“中央国家安全领导机构”的所指。	何为“中央国家安全领导机构”应该详细说明，并应明确决策过程是在中央一级管理，还是下放到省/地方一级。
7	各地区、各部门对本地区、本部门工作中产生、汇总、加工的数据及数据安全负主体责任。 工业、电信、自然资源、卫生健康、教育、国防科技工业、金融业等行业主管部门承担本行业、本领域数据安全监管职责。 公安机关、国家安全机关等依照本法和有关法律、行政法规的规定,在各自职责范围内承担数据安全监管职责。 国家网信部门依照本法和有关法律、行政法规的规定,负责统筹协调网络数据安全和相关监管工作。	1）不清楚“各地区、各部门”指的是哪一级政府，也不清楚这些部门是仅在本级别管辖数据活动，还是也负责下级开展的数据活动。 2）特定部门的行政部门和公安机关之间可能存在管辖重叠，这可能导致重复或多余监督。	我们建议 1）明确对数据进行权威监督的相关国家和地区机构的作用和责任。此外，澄清国家和地区机构将如何传达这些工作的准则和标准。 2）明确行业管理部门和公安机关之间的界限，避免执法和监督之间的冲突。

8	开展数据活动,必须遵守法律、行政法规,尊重社会公德和伦理,遵守商业道德,诚实守信,履行数据安全保护义务,承担社会责任,不得危害国家安全、公共利益,不得损害公民、组织的合法权益。	第八条提供了难以客观评估的高层次原则。这些宽泛的原则将带来合规挑战，并可能导致不同司法管辖区执法不一致。因此，草案应该提供具体的指导方针。	我们建议修改该条款，与草案第二十五条保持一致，因为第二十五条规定了可衡量的标准。
10	国家积极开展数据领域国际交流与合作,参与数据安全相关国际规则和标准的制定,促进数据跨境安全、自由流动。		令人鼓舞的是，该草案促进了数据相关事项的国际合作和交流、标准制定以及数据的自由流动。我们建议 1）中国发展跨境数据流动标准及法规的制定可优先考虑与现有国际框架和机制兼容。2）我们还鼓励根据《外商投资法》增加具体条款，以确保跨国公司平等参与标准制定过程。
11	任何组织、个人都有权对违反本法规定的行为向有关主管部门投诉、举报。收到投诉、举报的部门应当及时依法处理。		为了有效投诉或举报，必须明确本条所指的“有关主管部门”。此外，该条款应提供一个时间表，并就投诉的提交和反馈程序提供进一步指导。
第二章	数据安全与发展		
15	国家推进数据开发利用技术和数据安全标准体系建设。国务院标准化行政主管部门和国务院有关部门根据各自的职责,组织制定并适时修订有关数据开发利用技术、产品和数据安全相关标准。	1）我们总体认同制定标准对国内市场有利。 2）然而，我们希望指出，标准应当允许企业有必要的灵活性来满足具体行业的需求。 3）此外，企业注意到，法律法规引用的国家或行业推荐标准提出大量要求，但缺乏实	1）标准法规应基于风险，并允许各个组织根据其运营需求采取安全措施。 2）数据安全标准应尽可能最大限度地认可和采用国际标准，并在不可能完全采用的情况下尽量保持一致。 3）强制性要求应在法律法规中有明确规定，

	国家支持企业、研究机构、高等学校、相关行业组织等参与标准制定。	施细节。	不得通过直接引用其他法律法规的方式强迫公司采用推荐标准。
16	国家促进数据安全检测评估、认证等服务的发展,支持数据安全检测评估、认证等专业机构依法开展服务活动。		我们建议 1）该条应包含对外资企业平等对待，并包含允许自我评估和认证的条款。 2）应提供授权进行数据安全评估和认证的专门机构的明确清单。
17	国家建立健全数据交易管理制度,规范数据交易行为,培育数据交易市场。	尚不清楚统一数据交易市场的先例是什么，是否会有专门的法律法规来管理数据交易流程以及数据交易者的责任和义务。	我们建议制定专门的法律法规，为包括交易实体、内容和数据安全等在内的“数据交易市场”提供明确的规定。
第三章	数据安全制度		
19	国家根据数据在经济社会发展中的重要程度,以及一旦遭到篡改、破坏、泄露或者非法获取、非法利用,对国家安全、公共利益或者公民、组织合法权益造成的危害程度,对数 据实行分级分类保护。	1）企业担心，各省、各部门的重要数据目录因为地理管辖范围不同而不一致，也不符合《网络安全法》中现有的重要数据规定。 2）权力下放和授权给地方政府来制定各自的“重要数据”保护目录可能会导致与合规要求混淆，并对中国管辖范围内的数据自由流动造成障碍。 3）没有足够的细节来确定谁有权或使用什么标准来确定重要数据的范围。目前看来，地方政府将对“重要数据”拥有广泛的解释权。 4）国家的数据分级分类系统与各地区、各部门编制的重要数据目录有什么关系？ 6）鉴于企业使用的数据多种多样，重要数	我们建议 1）应明确“重要数据”的标准和目录制定流程，各地区的制定标准应保持一致。所有标准都应为外国公司提供意见征询期。 2）确定重要数据范围和定义的权力应限制在行业层面，并集中统一。 3）明确数据分级分类标准是否与现有行业/国家标准一致，如《工业数据分类分级指南》(试行)、《证券期货业数据分类分级指南》(JR/T 0158-208)、《金融数据安全数据安全分级指南 》(送审稿)等。 4）解释如何对多个行业中普遍的数据类型进行编目和分类。

		据目录的分类和分级系统显然不可行。 7）《数据安全管理办法》草案中定义的重要数据不包括与生产、运营和内部管理相关的个人信息或公司数据。草案会扩大这个范围吗？	
21	国家建立数据安全应急处置机制。发生数据安全事件,有关主管部门应当依法启动应急预案,采取相应的应急处置措施,消除安全隐患,防止危害扩大,并及时向社会发布与公众有关的警示信息。	1）不清楚这一规定是否确定了在国家/政府层面发生数据安全事故时国家应采取的措施，或者这是否适用于一般的数据安全事故。 2）该草案没有明确定义“数据安全事件”，并且在报告时间上含糊不清，这将影响企业履行报告相关事件的义务。	我们建议 1）应说明“数据安全事故”的定义和范围。 2）数据控制人员应根据国际标准(如 GDPR 标准)，在知晓后 72 小时内报告数据泄露。
22	国家建立数据安全审查制度,对影响或者可能影响国家安全的数据活动进行国家安全审查。 依法作出的安全审查决定为最终决定。	1）需要明确数据安全审查制度的关键细节，包括数据安全审查流程，哪些部门可以启动审查，审查时间表等。 2）不清楚将使用什么指南或标准来确定哪些数据活动将被视为对“国家安全”有影响。此外，数据活动的广泛定义增加了安全审查被广泛解释和用于预期范围之外的可能性。 3)政府参与商业数据活动应仅限于必要数据和对国家安全有最高影响的数据。	我们建议 1）数据安全审查仅限于已在最高保护级别正确编目和分类的重要数据。 2）提供对国家安全审查结果提出质疑并上报相关国家部委的机制。 3）解释数据安全审查如何与网络安全审查保持一致，以避免重叠。 4）就如何启动审查、哪些数据活动危害国家安全、谁是相关审查机构，以及审查机制的具体细节提供明确指引。
23	国家对与履行国际义务和维护国家安全相关的属于管制物项的数据依法实施出口管制。	受管制类别的定义和范围仍不清楚。	我们建议 1）明确哪些数据属于出口管制类别，以及具体的数据出口管制措施。与贸易领域的出口管制类似，与履行国际义务和维护国家安全有关的数据将被归类为受管制物项，因此需要在出

			口前获得许可。 2）解释本条款将如何与《个人信息出境安全评估办法》草案保持一致。
24	任何国家或者地区在与数据和数据开发利用技术等有关的投资、贸易方面对中华人民共和国采取歧视性的禁止、限制或者其他类似措施的,中华人民共和国可以根据实际情 况对该国家或者地区采取相应的措施。	目前尚不清楚对那些针对中国采取歧视性禁令的外国政府会采取何种报复措施。引发的报复措施可能影响外国企业。	我们建议删除该条款，并在更合适的法规(如《出口管制法》)中解决该问题。
25	开展数据活动应当依照法律、行政法规的规定和国家标准的强制性要求,建立健全全流程数据安全管理制度,组织开展数据安全教育培训,采取相应的技术措施和其他必要措施,保障数据安全。 重要数据的处理者应当设立数据安全负责人和管理机构,落实数据安全保护责任。		我们建议澄清数据安全负责人的必备资格，以及这一角色是否可以在中国境内的母公司和子公司之间共享。
第四章	数据安全保护义务		
28	重要数据的处理者应当按照规定对其数据活动定期开展风险评估,并向有关主管部门报送风险评估报告。		我们建议 1）提供重要数据和重要数据处理者的清晰定义。 2）将重要数据安全评估限制在最高级别明确

	风险评估报告应当包括本组织掌握的重要数据的种类、数量,收集、存储、加工、使用数据的情况,面临的数据安全风险及其应对措施等。		识别的数据。 3）将需要风险评估的活动范围限制在重要数据处理活动，而不是可能拥有重要数据的主体。
29	任何组织、个人收集数据,必须采取合法、正当的方式,不得窃取或者以其他非法方式获取数据。 法律、行政法规对收集、使用数据的目的、范围有规定的,应当在法律、行政法规规定的目的和范围内收集、使用数据,不得超过必要的限度。	何为本条提及的“正当的方式”。=	我们建议删除“正当的方式”。“合法方式”足以表达本条的意图。
30	从事数据交易中介服务的机构在提供交易中介服务时,应当要求数据提供方说明数据来源,审核交易双方的身份,并留存审核、交易记录。	不清楚数据提供方需要采取什么措施来“说明数据来源。”尚不清楚是否还需要中介服务来验证交易中的数据来源。	我们建议明确数据交易中介服务机构资质、权限、定义等。
31	专门提供在线数据处理等服务的经营者,应当依法取得经营业务许可或者备案。具体办法由国务院电信主管部门会同有关部门制定。	本条的“在线数据处理”服务与 2015 年《电信业务分类目录》在线数据处理服务定义的关系尚不清楚。	我们建议为在线数据处理服务提供一个明确的定义，说明如何与 2015 年《电信业务分类目录》中的定义保持一致。
32	公安机关、国家安全机关因依法维护国家安全或者侦查犯罪的需要调取数据,应当按照国家有关规定,经过严格的批准手续,依法进行,有关组织、个人应当予以配	1）不清楚本条所指的“手续”是什么。 2）在实践中，主管部门经常要求企业提供保密数据。然而，一些部门不提供书面通知，仅提供口头通知。这迫使企业陷入两难境地，它们必须非法向有关部门提供数据，	我们建议 1）提供附录或表格或公众可访问的网站，公布第 32 条授权的国家、地区和行业监管机构及联系人。 2）明确监管机构向企业索要数据的范围和限

	合。	否则将承担违规的后果。	制。应包括保护组织和个人的合法权益。 3）增加关于国家机关数据安全责任的条款。
33	境外执法机构要求调取存储于中华人民共和国境内的数据的,有关组织、个人应当向有关主管机关报告,获得批准后方可提供。中华人民共和国缔结或者参加的国际条约、协定对外国执法机构调取境内数据有规定的,依照其规定。	境外执法机构的定义和范围不明确，例如是否包括境外司法机关、税务局、证券交易所、清算所等。 只有经监管机构批准才能提供的数据范围是什么？在这些情况下，谁是相关主管部门？如果管辖权重叠怎么办？	我们建议 1）明确“境外执法机构”的范围，以及需要国家、地区或部门审查的数据类型。 2）限制应要求提供给执法部门的数据范围。 3）提供有关程序、决策和主管部门时间表的更详细规定。
第六章	法律责任		
46	履行数据安全监管责任的国家工作人员玩忽职守、滥用职权、徇私舞弊,尚不构成犯罪的,依法给予处分。	本文中的“国家工作人员”是指专门负责数据安全的政府工作人员，还是监督所有组织和个人的工作人员？ 如果是后者，则有必要增加一条保护商业秘密和专有信息的条款，并在发生侵犯商业秘密或专有信息并给企业造成损失的情况下，提供刑事责任之外的民事赔偿。	建议将该条修改为：“履行数据安全监管职责的国家工作人员玩忽职守、滥用职权、侵犯商业秘密或者其他专有信息，或者滥用职权谋取私利，尚不构成犯罪的，依法给予处罚，并对侵犯商业秘密和专有信息的行为承担民事赔偿责任。”
47	通过数据活动危害国家安全、公共利益,或者损害公民、组织合法权益的,依照有关法律、行政法规的规定处罚。	见对第 3 条的评论	建议删除该条款。