THE US-CHINA BUSINESS COUNCIL
美 中 贸 易 全 国 委 员 会

美中贸易全国委员会关于《网络安全审查办法（修订草案征求意见稿）》的反馈意见

美中贸易全国委员会（下称我委员会）谨代表 250 余家会员企业就《网络安全审查办法（修订草案征求意见稿）》（下称“修订稿”）向国家互联网信息办公室提出意见。

首先，我委员会高度认可，确保信息与通信技术领域关键信息基础设施供应链的安全、维护国家安全，是所有国家的正当关切。《网络安全审查办法》作为《中华人民共和国网络安全法》的重要配套施行办法，为中国政府通过网络安全审查排除国家安全隐患提供了关键指导。

可是不得不承认，当前中国网络安全领域的法规体系已经较为复杂。在此基础上，本次发布的修订稿可能会进一步增加了不明确性和企业合规要求。与上一版本相比，修订稿的部分条文经过修订后反而不够明确；同时也明显扩大了可能涉及国家安全风险的行为范围，让非关键信息基础设施运营者承受不必要的负担。

诚然，对信息与通信技术产品和服务进行监管并非易事。我委员会期待中国政府对网络安全审查的实施保持在必要的最小范围，并保持审查标准的一致性。本次反馈意见中的重点内容如下：

1. **将审查对象限定为关键信息基础设施运营者：**根据修订稿，除了关键信息基础设施运营者，如果数据处理者的数据处理活动影响国家安全，也要接受网络安全审查。我委员会在之前提交的《中华人民共和国数据安全法》反馈意见中，已经明确指出，“数据处理活动”是一个过于宽泛的定义——企业无法据此预知哪些活动会触发安全审查机制。这样宽泛的定义增加了企业面临的不确定性，为企业合规设置了诸多挑战。在这种情况下，执法机构也很难做到基于规则执法、保证执法一致性。此外，修订稿没有明确区分“关键信息基础设施运营者”和“非关键信息基础设施运营者”，加剧了企业合规的复杂性。我委员会建议保留原《网络安全审查办法》中第一条的表述，将安全审查的对象限定为关键信息基础设施运营者。

2. **不将个人信息作为审查赴国外上市企业的条件：**将是否掌握个人信息作为申报审查的条件，再根据审查结果决定企业能否赴海外交易所上市，不符合国际规范。此举既不能有效规避安全风险，也会阻碍中国科技的发展。据我委员会了解，没有任何一个国家的现存法规将个人信息作为审查赴国外上市企业的条件。并且，美国也没有任何法规仅仅因为中国企业在美国上市就向这些中国企业强制索取其在中国收集的数据。对于中国企业而言，赴美上市是重要的募资渠道，是未来实现技术创新、开拓国际市场的动力来源。因此，为企业赴美上市设置这样的阻碍可能会对中国的技术进步有所影响。

3. **以信息风险评估替代个人信息数量作为审查前提：**根据修订稿，掌握超过 100 万用户个人信息的运营者赴国外上市，必须向网络安全审查办公室申报网络安全审查。我委员会及会员企业坚决反对基于信息的数量制定合规要求：因为一个企业收集、掌握的信息量并不能作为风险评定的指标。不同企业收集的个人信息种类各异，风险高低不同，一部分个人信息的来源甚至只是用户在网上主动公开的内容。因此，我委员会建议监管部门引入信息风险评估机制，替代个人信息的数量作为审查前提。

4. **厘清关键术语：**修订稿指出，监管部门需要依据本法特别保护“核心数据”和“重要数据”。但是，这两个术语缺乏准确定义，涉及这两个概念的相关规定也不易执行。对企业而言，无法准确理解条文中规定的义务，合规自然就会变得更加困难。

5. **确保公正执法：**我委员会高度认可《网络安全审查办法》的客观性。但与此同时，我们必须指出，本次修订稿中关于网络安全审查的规定可能会让跨国运营的企业（不管是外资跨国企业还是正在开拓全球市场的中国企业）负担过重，甚至面临政治和非贸易方面的风险。过去，美国企业为中国发展信息与通信技术供应链做出了重要贡献。未来，美企仍希望能与中方友好合作，共同攻克科技难关。

如条件允许，我委员会期待与国家互联网信息办公室就本次反馈开展进一步沟通，为中国政府防范国家安全风险、构建网络安全法律监管框架做出更多贡献。详细的建议信后附上。

美中贸易全国委员会北京代表处

2021 年 07 月 23 日

反馈意见汇总表			
条/款	**条/款内容**	**意见**	**建议**
第一条	为了确保关键信息基础设施供应链安全，维护国家安全，依据《中华人民共和国国家安全法》《中华人民共和国网络安全法》《中华人民共和国数据安全法》，制定本办法。	“为了确保关键信息基础设施供应链安全”的定义需要完善。	本办法后文中关于安全审查义务并未明确限定为“关键基础设施及相关供应链”，因此导致本办法适用范围前后不一致，容易引起误解。
第二条	关键信息基础设施运营者（以下简称运营者）采购网络产品和服务，数据处理者（以下称运营者）开展数据处理活动，影响或可能影响国家安全的，应当按照本办法进行网络安全审查。	1. 本草案将审查办法的适用范围从关键信息基础设施运营者采购网络产品和服务扩大到全部数据处理者开展数据处理活动。扩大的适用范围非常宽泛，除了（1）现有的关键信息基础设施运营者采购网络产品和服务和（2）国外上市这两种情形外，在草案中没有设定明确的标准规定网络安全审查应在符合什么门槛要求时被触发。对所有未落入上述两种情形的数据处理者而言，这就带来了很大的不确定性，不知道是否需要进行网络安全审查，也不知道是否需要申报审查。所以，仅概括性的规定“影响或可能影响国家安全”的数据处理活动应进行网络安全审查是不够的，应对此进行具体规定何为“影响或可能影响国家安全”。还有，跨国公司使用全球系统管理并在中国境外处理中国公民数据的是否属于此范围？ 2. 审查对关键信息基础设施运营者的要求和对其他数据处理者的要求是不同的。采购网络产品和服务的审查要求是仅针对关键信息基础设施运营者，而非普遍适用于所有数据处理者。但这两者在草案中是被统一定义为“运营者”，而且在下文的相关规定中并未区别对待，	1. 建议明确触发网络安全审查的具体条件和门槛，以使所有数据处理者可充分了解并遵守。 2. 建议将适用于不同身份（关键信息基础设施运营者、到国外上市的公司、普通数据处理者）分别定义，并分别列明对他们不同的审查条件和审查重点。比如，可以将“关键信息基础设施运营者”定义成“关键运营者”，将“数据处理者”定义成“一般运营者”，并将“关键运营者”和“一般运营者”统称为“运营者”。 3. 建议将“数据处理者开展数据处理活动”修改为“在中国境内合法注册登记的数据处理者在境内开展数据处理活动”。 4. 建议明确定义“数据处理者”和“数据处理活动”。“数据处理者”在本办法中应为有权自主决定数据处理目的和处理方式的组织或个人，而非受委托方。

		如第 5 条和第 7 条。这会在执法和守法时发生误认，增加非关键信息基础设施运营者不必要的合规负担。 3. 何为“数据处理者”以及“数据处理活动”在此并不明确。理解这两个定义对网络安全审查的适用范围十分关键。在《个人信息保护法（二审稿）》第七十二条定义了“个人信息处理者”（该定义与通用数据保护条例 GDPR 中关于数据控制者（data controller）的定义类似，即有权自主决定个人信息处理目的和处理方式的人，这与《信息安全技术-个人信息安全规范》第 3.1 条定义的“个人信息控制者”一致），第 22 条规定了“受托方”，类似于通用数据保护条例 GDPR 中定义的“数据处理者”（data processor，即受他人委托并为他人处理数据的一方）。在此，并不明确这些定义是否与本办法的定义一致，特别在处理“核心数据”和“重要数据”时，应如何适用。	
第五条	运营者采购网络产品和服务的，应当预判该产品和服务投入使用后可能带来的国家安全风险。影响或者可能影响国家安全的，应当向网络安全审查办公室申报网络安全审查。 关键信息基础设施保护工作部门可以制定本行业、本领域预判指南。	1. 对于数据处理者的预判依据和范围没有很明确的描述和指导。它可能会挑战全球部署战略和流程，包括中国境外的系统。虽然我们支持制定基于风险的行业准则和现有的公共/私人框架，以防止网络威胁。我们不赞成不必要的强制性或基于制裁的安全措施，这些措施会降低对网络安全的持续投资。 2. 对于采购网络产品与服务的审查的具体流程、频次及要求仍需要进一步明确。 3. 正如对第二条的评价，对采购网络产品和服务进行网络安全审查仅针对关键信息基础设施运营者，而非其他数据处理者。所以，这条应写清适用对象，而非统一称之“运营者”。	建议这两条中以“关键信息基础设施运营者”（或如建议中用“关键运营者”）替代“运营者”。 对于采购的网络产品与服务建议按照《网络关键设备和网络安全专用产品目录》的形式予以确认。

第六条	掌握超过 100 万用户个人信息的运营者赴国外上市，必须向网络安全审查办公室申报网络安全审查。	需要明确界定“运营者”的范围和“国外”的定义。比如： 1）“运营者”仅指中华人民共和国的运营者，还是包含其他国家或地区(如：港、澳、台,等)？ 2）上市的范围不清晰(如：赴香港上市是否包含在此条款中,还有国外，上市有什么定义和范围)？ 3）已经在国外上市的跨国公司在中国境内注册的子公司/关联公司之间的数据跨境传输是否在此条款范围?	建议明确界定“运营者”的范围和上市国家或地区的范围，以避免错误理解。 这里个人信息超过 100 万的运营者赴国外上市，须接受网络安全审查。对于一些跨国公司的子公司/关联公司之间的数据跨境传输，建议提供明确的定义和管理办法，以及范围。 此外，建议明确向网络安全办公室的申报时间范围，涉及第一次申报以及已经上市须重新申报的两类时间点。
第八条	运营者申报网络安全审查，应当提交以下材料： （二）关于影响或可能影响国家安全的分析报告； 	需要明确清晰的分析报告内容和评估依据。是否每个合同（如采购）都可能触发安全审查申请？若有多项类似合同，是否可集中申请？	建议明确只有依照本办法第 5 条关键信息基础设施运营者采购网络产品和服务以及第六条数据处理者赴海外上市才必须申报审查。 建议制定分析报告模板或指南来指导运营者进行评估和分析，以避免错误理解。
第十条	网络安全审查重点评估采购活动、数据处理活动以及国外上市可能带来的国家安全风险，主要考虑以下因素： （五）核心数据、重要数据或大量个人信息被窃取、泄露、毁损以及非法利用或出境的风险； （六）国外上市后关键信息基础设施，核心数据、重要数据或大量个人信息被国外政府影响、控制、恶意利用的风险；	在此条款中的 “核心数据”和“重要数据”的定义不清晰，以及哪些信息将被视为“大量”个人信息的范围不明确。 针对不同的情形，审查因素是不一样的，比如我们理解本条所列的因素（一）至（四）应该是针对关键信息基础设施运营者的采购活动，而（五）是针对数据处理活动，（六）是针对国外上市。 若此理解无误，建议本条中将此分开列明，以避免在执法和实务中产生误解。	1. 建议明确定义核心数据和重要数据以及界定个人信息数量的范围，以避免造成混淆和定义不一致。 2. 特定的网络安全要求适用于特定行业，我们建议使用明确的术语和定义来识别和分类核心数据和重要数据，以确保对真正重要的特定行业的数据进行此类处理。 3. 建议明确因素（一）至（四）应该是针对关键信息基础设施运营者的采购活动，而（五）是针对数据处理活动，（六）是针对国外上市。

			4. 针对“个人信息”，无论在《民法典》还是在《个人信息保护法》（草案）中，对公开和非公开的个人信息有不同的规定。一般而言，合法公开的个人信息和非敏感个人信息并不会对国家安全造成影响，也没有进行网络审查的必要。故此，建议在本条所列因素（五）和（六）中将“个人信息”限制在非公开个人信息范围内。
第十四条	特别审查程序一般应当在3个月内完成，情况复杂的可以延长。		若无要求提供补充材料或无特别审查程序，每次审查时间约3个月，若案情复杂，则可能审查时间更久。建议缩短相应的审查时间。
第二十一条	本办法中关键信息基础设施运营者是指经关键信息基础设施保护工作部门认定的运营者。 本办法所称网络产品和服务主要指核心网络设备、重要通信产品、高性能计算机和服务器、大容量存储设备、大型数据库和应用软件、网络安全设备、云计算服务，以及其他对关键信息基础设施安全有重要影响的网络产品和服务。	“关键信息基础设施”及其他关于“核心网络”“重要通信产品”“高性能、大容量、大型”等表述需要进一步完善定义与适用范围。	提高法律的确定性，以减少适用中的歧义与疑问。 明确定义“网路产品和服务”，以避免造成混淆和定义不一致。