Confidential – FOR USITO MEMBERS ONLY

美国信息产业机构
United States Information Technology Office

2018 年 7 月 27 日

谨致：中华人民共和国公安部
抄送：中华人民共和国国家互联网信息办公室

关于：美国信息产业机构关于《网络安全等级保护条例（征求意见稿）》的意见和建议

尊敬的公安部领导：

美国信息产业机构（USITO）感谢有机会就**公安部 2018 年 6 月 27 日发布的《网络安全等级保护条例（征求意见稿）》**（条例草案）提出我们的意见和建议。USITO 代表全球信息通信技术（ICT）行业处于领先地位的一批大型创新企业，其中很多企业在中国拥有长期投资，并积极致力于促进中国经济和 ICT 产业可持续发展。USITO 秉承一贯的目标，在协助公安部在实现其公共政策目标的同时，努力确保政策的实施不给商业机构的商业活动带来过重的监管性负担。由衷希望我们的意见和建议得到贵部的深入考量，并希望有机会在条例后续修订和征求意见过程中继续贡献我们的意见和看法。

我们赞赏公安部积极采取明智灵活的政策、建立均衡、全面的网络安全防护制度的努力，这对于满足中国当前的网络安全防护需求是适宜的。然而，在公安部发布的这份条例征求意见稿中，只规定了达到结果的手段，而没有明确需要达到何种结果。草案扩大了现有的由 2007 年颁布的《信息系统等级保护管理办法》建立的等级保护制度，列出一套严格的规定，要求 ICT 行业遵照执行，对行业提出了一系列硬性且繁琐的要求，但实际上这些规定和要求并不必然会带来网络安全的提升，或达到预定的网络安全目标。贵部起草的这份条例草案还将导致行业产生不必要的混淆和担忧，有可能与其上位法《网络安全法》相互冲突。具体问题详述如下：

- 条例征求意见稿扩大了网络安全等级保护制度的涵盖范围并降低了网络安全等级保护三级的门槛。首先，此条例征求意见稿远远超出 2007 年发布的信息安全等级保护管理办法的范围，从信息系统扩展到了网络基础设施安全、网络运行安全、数据安全和信息安全，并突出了对现有以及新兴技术（例如人工智能等技术）的管控。我们建议等保条例遵循上位法网络安全法，避免扩大范围，不必要的增加监管事项。其次，条例第一次将重要的，一旦破坏可能对公民、法人和其他组织的合法权益造成特别严重损害的系统定级为三级，这将创造一个令人担忧的先例。根据

北京市朝阳区太阳宫中路 12 号太阳宫大厦 1104 室 邮编：100028
联系电话：（86-10）8429-9070 传真：（86-10）8429-9075

2007 年发布的信息安全等级保护管理办法，涉及到国家安全的系统定义为三级。现有条例将涉及到个人和组织利益的商用市场所覆盖的范围一并和国家安全的重要性等同，不仅级大扩大了三级的范围，把若干增长迅猛、前景广阔的 ICT 市场囊括在内。这样的范围扩大对保护国家安全真正重要的网络无益，可能造成浪费稀缺的公共资源，并过多介入商用市场。

- 条例草案引入了不合理的要求，大幅度增加了企业应履行的工作和义务，扩展了日志保存的范围，对运营者提出了大量要求，如备案、审核、检查、检测、测评等等。以第三级网络为例，草案规定，三级网络的运营者应当和同级公安机关对接。我们希望强调一点，公安机关在任何情况下都不应介入企业网络，这样严格的要求没有效果而且徒增网络安全以及用户隐私风险。此外，条例草案规定三级网络运营者应当每年开展一次网络安全等级测评，每年对本单位落实网络安全等级保护制度情况和网络安全状况至少开展一次自查，组织密码应用安全性评估，并接受公安机关的检查。如果系统涉及个人信息和/或重要数据出境等情况，需要开展年度评估，其重要性超过定期自查和可能开展的监管性评估。如果系统被认定为关键信息基础设施（CII），则需要面对另一套几乎完全相同的检查和评估规定，这套规定即 2017 年 7 月发布的《关键信息基础设施安全保护条例（征求意见稿）》（以下简称 CIIP 条例）。除此以外，条例草案还要求运营者获得其他行政审批许可，例如第 21 条规定的网络安全职业资格证书。草案提出的这些具有强制性、范围广泛的报告和合规要求不利于运营者的业务运营。对运营者强制实施这些要求，往往会促使运营企业把宝贵的稀缺资源集中用于执行那些仅涵盖已知漏洞的具有可追溯性的核查对照表，而不是在一个动态变化的威胁环境中主动应对解决不断升级的风险。

- 条例草案对运营者规定的新增义务和管理方面的工作负担也远远超出了《网络安全法》规定的范围，而这份草案正是依据后者制定的。与此同时，条例草案在其他方面的一些规定与《网络安全法》里的对网络关键设备以及网络安全专用产品的检测和认证制度以及与网络安全审查制度的关系不明确。为了避免重复以及进行不必要的规定，我们建议草案明确说明各种制度的依据和必要性 。这样有助于草案认真履行国务院提出的简化减少政府审批程序的改革精神，包括减少资质资格许可认定

和行政许可审批事项等等。[1, 2]

- 还需要指出的是，本条例草案与 CIIP 条例草案一些内容存在不一致的情况，后者依据《网络安全法》正在制定中，其对关键信息基础设施提出的保护要求与本条例略有不同。这种要求上的出入将给行业带来困惑，还会导致不必要地增加运营者为满足两套规定而产生的合规成本。

- 除了《网络安全法》与 CIIP 条例草案存在明显的冲突之外，本条例草案中一些条款表述用词宽泛，不仅增加了合规难度，还给企业增加了不确定性，加深了其对知识产权和数据隐私保护问题的担忧。此外，很多公司不清楚公安部对“新技术”等术语如何定义，会要求公司采取哪些措施管控安全风险。如果不进一步明确这些问题，本条例草案条款就有可能在无意间对知识产权和数据隐私保护形成阻碍。

为了有效保护网络安全，切实解决上述问题，同时促进全球联通，USITO 建议对本条例草案重新起草，重点强调需要达到的网络安全结果和应当实施的原则，以便行业企业将其贯穿在所采取的网络防护措施中。如此，不仅能保证条例草案不超出《网络安全法》的范围，而且与 CIIP 条例草案规定及国务院简化减少政府审批程序的改革精神保持一致。

最后，本条例草案应当与其它规定了复杂网络安全义务的政策法规一样，应豁免在条例正式颁布前建设的网络，给在建网络至少一年的实施宽限期，以便公司能实现逐步过渡，为实施新条例做好准备。这个宽限期应当在条例草案中明确予以规定。同时，合规检查等工作应在条例以及配套细节正式发布后再进行。

鉴于本条例草案对中国境内企业将会产生广泛深远的影响，且其影响程度很可能超出起草机构的预计，我们希望，在条例正式实施之前能够有机会对其今后发布的征求意见稿继续进行探讨，并提出我们的意见和建议。USITO 愿意在公安部制定和完善其法规和政策

1 《立法法》（2015 版）第八十二条规定：没有法律、行政法规、地方性法规的依据，地方政府规章不得设定减损公民、法人和其他组织权利或者增加其义务的规范。

2 《立法法》（2015 版）第八十条规定：部门规章规定的事项应当属于执行法律或者国务院的行政法规、决定、命令的事项。没有法律或者国务院的行政法规、决定、命令的依据，部门规章不得设定减损公民、法人和其他组织权利或者增加其义务的规范，不得增加本部门的权力或者减少本部门的法定职责。

的过程中，随时提供必要的协助，同时努力推动企业创新和成长的大环境不断走向完善。感谢认真考虑我们的意见。

美国信息产业机构（USITO）

我们对条例草案具体条款的意见和建议详见下表：

条款号	原文	修改建议	意见
1	【立法宗旨与依据】为加强网络安全等级保护工作，提高网络安全防范能力和水平，维护网络空间主权和国家安全、社会公共利益，保护公民、法人和其他组织的合法权益，促进经济社会信息化健康发展，依据《中华人民共和国网络安全法》、《中华人民共和国保守国家秘密法》等法律，制定本条例。	建议明确本条中包括的一些法律术语。	本条例中有多处措辞含糊不清（如“社会公共利益”和“信息化健康发展”）。如果定义不清晰，业界很难准确理解上述术语的具体要求。
2	【适用范围】在中华人民共和国境内建设、运营、维护、使用网络，开展网络安全等级保护工作以及监督管理，适用本条例。个人及家庭自建自用的网络除外。	建议把适用范围缩小至政务网络。	本条例草案适用范围太过宽泛，可能适用于所有商用网络。
6	【网络运营者责任义务】网络运营者应当依法开展网络定级备案、安全建设整改、等级测评和自查等工作，采取管理和技术措施，保障网络基础设施安全、网络运行安全、数据安全和信息安全，有效应对网络安全事件，防范网络违法犯罪活动。	建议划线处修改为： “保障网络基础设施安全、网络运行安全、数据安全~~和信息安全~~”	本条内容应与第四条保持一致。
9	【标准制定】国家建立完善网络安全等级保护标准体系。国务院标准化行政主管部门和国务院公安部门、国家保密行政管理部门、国家密码管理部门根据各自职责，组织制定网络安全等级保护的国家标准、行业标准。 国家支持企业、研究机	建议修改为： “【标准制定】国家建立完善网络安全等级保护标准体系。国务院标准化行政主管部门和国务院公安部门、国家保密行政管理部门、国家密码管理部门根据各自职责，组织制定网络安全等级保护的国家标准~~、行业标准~~。	鉴于配合规章实施的标准非常重要，这些标准如果按行业割裂开来，会造成实施上的一定风险。因此，应当均为国家标准。

	构、高等学校、网络相关行业组织参与网络安全等级保护国家标准、行业标准的制定。	国家支持企业、研究机构、高等学校、网络相关行业组织参与网络安全等级保护国家标准~~、行业标准~~的制定。”	
10	【投入和保障】各级人民政府鼓励扶持网络安全等级保护重点工程和项目，支持网络安全等级保护技术的研究开发和应用，推广安全可信的网络产品和服务。	建议删除“推广安全可信的网络产品和服务”的表述，因为此句在一些情况下被理解为鼓励购买国产产品。	“安全可信”的说法在过去一直沿用，含蓄地表明了对国产产品的偏爱；由此而形成的制度还要求对外国产品进行侵入式检测，但这种检测方式有可能导致知识产权信息面临泄露风险。
14	【鼓励创新】国家鼓励利用新技术、新应用开展网络安全等级保护管理和技术防护，采取主动防御、可信计算、人工智能等技术，创新网络安全技术保护措施，提升网络安全防范能力和水平。	建议修改为： “【鼓励创新】国家鼓励利用新技术、新应用开展网络安全等级保护管理和技术防护，~~采取主动防御、可信计算、人工智能等技术，~~创新网络安全技术保护措施，提升网络安全防范能力和水平。”	由于技术的发展日新月异，在条例草案中指定采用具体技术似乎欠妥。
15	（三）第三级，一旦受到破坏会对相关公民、法人和其他组织的合法权益造成特别严重损害，或者会对社会秩序和社会公共利益造成严重危害，或者对国家安全造成危害的重要网络。	建议修改为： “第三级，一旦受到破坏会对~~相关公民、法人和其他组织的合法权益造成特别严重损害，或者会对~~社会秩序和社会公共利益造成严重危害，或者对国家安全造成危害的重要网络。”	依据 2007 年发布的《信息系统等级保护管理办法》（我们理解其将被本条例草案规定的网络安全等级保护制度取代）， 对于三级或以上网络，一旦发生泄漏事件，将对“社会秩序和公共利益造成严重危害或对国家安全造成危害”。公民、法人和其他组织可以通过民事和刑事措施保护其合法权益，因此，使三级至五级网络仅仅与社会秩序、社会公共利益和国家安全关联起来是最佳判定手段 （即恢复其最初的定义）。如果扩大三级网络的关联范围，将使企业的合规负担显著增加，因为三级网络需要进行检测认证。在这个规定严格的等级保护体系中，三级是一个关键性级别，应当仅限于某些具体行业，这也符合当初建立等级保护制度的初衷。 此外，哪些情况构成对社会秩序和社会公共利益造成“严重危害”，草案没有给出明确定义。
16	【网络定级】**网络运营者**应当在规划设计阶段确定网络的安全保护等级。 当网络功能、服务范围、服务对象和处理的	建议明确何种情况构成“重大变化”。此外，建议制定详细的网络定级标准，使运营者能准确定级。	建议公安部明确说明，变更安全保护等级是否需要有资质的第三方参与。

	数据等发生重大变化时，网络运营者应当依法变更网络的安全保护等级。		
17	【定级评审】对拟定为第二级以上的网络，其运营者应当组织专家评审；有行业主管部门的，应当在评审后报请主管部门核准。 跨省或者全国统一联网运行的网络由行业主管部门统一拟定安全保护等级，统一组织定级评审。 行业主管部门可以依据国家标准规范，结合本行业网络特点制定行业网络安全等级保护定级指导意见。	建议制定详细的网络运营者自我评审规定，包括针对专家选择和专家评审程序提出明确要求。 建议本条例应“依据国际标准规范”，而不是“依据国家标准规范”。 建议从第三级网络开始要求组织“专家评审”。	本条内容与标准草案《信息安全技术　网络安全等级保护定级指南》第 5.2 条冲突。后者规定，“跨省业务专网可作为一个整体对象定级，也可以分区域划分为若干个定级对象”（而不是确定一个统一的安全保护等级）。 此外，本条要求对拟定为第二级以上的网络，其运营者应当组织专家评审；为何是从二级开始，条例中没有说明原因。
18	【定级备案】第二级以上网络运营者应当在网络的安全保护等级确定后10个工作日内，到县级以上公安机关备案。 因网络撤销或变更调整安全保护等级的，应当在10个工作日内向原受理备案公安机关办理备案撤销或变更手续。 备案的具体办法由国务院公安部门组织制定。	建议对现有网络实施豁免，现有网络的建设是符合建设时期的各种规定要求，如强制要求现有网络按照要求整改，可能导致整体的系统迁移，给企业带来沉重的负担。 建议对现有网络给予豁免，并在备案程序方面实施实施宽限期，以便运营者完成备案程序。	
20	【一般安全保护义务】网络运营者应当依法履行下列安全保护义务，保障网络和信息安全： （一）确定网络安全等级保护工作责任人，建立网络安全等级保护工作责任制，落实责任追究制度； （二）建立安全管理和	建议本条修改为： “【一般安全保护义务】网络运营者应当依法履行下列安全保护义务，保障网络和信息安全： （一）确定网络安全等级保护工作责任人，建立网络安全等级保护工作责任制，落实责任追究制度；	建议明确本条第（四）项中“身份识别”一词的含义，明确哪些人的身份需要识别。另外，建议删除第（五）项内容，采用《网络安全法》中的 “网络日志”留存规定，因为此处的规定超出了《网络安全法》的要求。 此外，《网络安全法》第五十条规定，“国家网信部门和有关部门依法履行网络信息安全监督管理职责，发现法律、行政法规禁止发布或者传输的信息的，应当要求网络运营者停止传输”。基于此，我们建议删除第（八）项中的“发现”一词，因为依据《网络安全法》，这不属于网络运营者的义务；否则，就相当于把

	技术保护制度，建立人员管理、教育培训、系统安全建设、系统安全运维等制度； （三）落实机房安全管理、设备和介质安全管理、网络安全管理等制度，制定操作规范和工作流程； （四）落实身份识别、防范恶意代码感染传播、防范网络入侵攻击的管理和技术措施； （五）落实监测、记录网络运行状态、网络安全事件、违法犯罪活动的管理和技术措施，并按照规定留存六个月以上可追溯网络违法犯罪的相关网络日志； （六）落实数据分类、重要数据备份和加密等措施； （七）依法收集、使用、处理个人信息，并落实个人信息保护措施，防止个人信息泄露、损毁、篡改、窃取、丢失和滥用； （八）落实违法信息发现、阻断、消除等措施，落实防范违法信息大量传播、违法犯罪证据灭失等措施； （九）落实联网备案和用户真实身份查验等责任； （十）对网络中发生的案事件，应当在二十四小时内向属地公安机关报告；泄露国家秘密	（二）建立安全管理和技术保护制度，建立人员管理、教育培训、系统安全建设、系统安全运维等制度； （三）落实机房安全管理、设备和介质安全管理、网络安全管理等制度，制定操作规范和工作流程； （四）落实身份识别、防范恶意代码感染传播、防范网络入侵攻击的管理和技术措施； ~~（五）落实监测、记录网络运行状态、网络安全事件、违法犯罪活动的管理和技术措施，并按照规定留存六个月以上可追溯网络违法犯罪的相关网络日志；~~ （五）落实监测、记录网络运行状态和网络安全事件的技术措施，并按照规定留存六个月以上的相关网络日志 （六）落实数据分类、重要数据备份和加密等措施； （七）依法收集、使用、处理个人信息，并落实个人信息保护措施，防止个人信息泄露、损毁、篡改、窃取、丢失和滥用； （八）落实违法信息~~发现、~~阻断、消除等措施，落实防范违法信息大量传播、违法犯罪证据灭失等措施； （九）落实联网备案和	识别非法信息和搜集网络违法犯罪证据的工作负担放在网络运营者身上，超出了《网络安全法》的要求。网络运营者并不是承担这一任务的最佳选择。 对于本条第（十）项，我们建议报告义务应当仅限于三级和以上网络，仅针对网络运营者已知或刚发现的严重事件。报告时限规定为 72 小时，是针对这类安全事件的全球通用规范 最后一点，由于中文的“案事件”一词包括了事件和法律案件，该词必须进一步明确。

	的，应当同时向属地保密行政管理部门报告。 （十一）法律、行政法规规定的其他网络安全保护义务。	用户真实身份查验等责任； （十）对第三级或以上网络中发生的网络运营者已知或已经发现的严重案事件，应当在网络运营者开始知晓或发现~~三十四~~七十二小时内向属地公安机关报告；泄露国家秘密的，应当同时向属地保密行政管理部门报告。 （十一）法律、行政法规规定的其他网络安全保护义务。”	
21	【特殊安全保护义务】第三级以上网络的运营者除履行本条例第二十条规定的网络安全保护义务外，还应当履行下列安全保护义务：… （二）制定并落实网络安全总体规划和整体安全防护策略，制定安全建设方案，并经专业技术人员评审通过； … （三）对网络安全管理负责人和关键岗位的人员进行安全背景审查，落实持证上岗制度；… （五）落实网络安全态势感知监测预警措施，建设网络安全防护管理平台，对网络运行状态、网络流量、用户行为、网络安全案事件等进行动态监测分析，并与同级公安机关对接；	建议修改为： “【特殊安全保护义务】第三级以上网络的运营者除履行本条例第二十条规定的网络安全保护义务外，还应当履行下列安全保护义务：… ~~（二）制定并落实网络安全总体规划和整体安全防护策略，制定安全建设方案，并经专业技术人员评审通过；~~… （五）落实网络安全态势感知监测预警措施，建设网络安全防护管理平台，在依法保护个人信息、私人信息和商业秘密的前提下，对网络运行状态、网络流量、用户行为、网络安全案事件等进行动态监测分析~~，并与同级公安机关对接~~；”	希望明确本条第（五）项对接一词的含义。这种对接是指与公安部专门联络的人员定期报告或备案，还是指实时的系统与系统连接？如果要求与网络运营者系统建立技术连接，这项要求将会严重打扰企业的正常运营。这种与公安机关建立的不受约束的连接，将使网络运营者和用户极难确定其隐私、专有信息和合法利益是否能得到有效保护。 《网络安全法》还规定，网络运营者应对公安机关提供技术支持和协助。本条例草案应避免扩大《网络安全法》所确定的范围，不应允许主管机关过多地访问网络运营者网络。基于上述原因，我们认为，要求所有的三级以上系统“与公安机关对接”将给运营者带来巨大的负担。这一要求应当删除，或仅限于人员联络。 此外，由于三级网络认证检测和年度网络等级测评已涵盖了第（二）项所述要求，我们建议删除第（二）项内容。这将有助于减少法人实体的合规负担，且不影响网络安全。 第（三）项所述的“安全背景审查”内容不清晰，建议给予详细说明。
22	【上线检测】新建的第二级网络上线运行前应当按照网络安全等级保护有关标准规范，对网络的安全性进行测试。	为了避免重复，建议明确本条例和《网络安全法》之间安全测评的工作范围划分。此外，建议明确安全等级测评应	如果网络产品或服务已通过《网络安全法》规定的安全审查，其是否还要再次接受测试？等级保护条例和《网络安全法》之间是什么关系？如果需要再次测试，则本规定将会造成重复许可的问题，这将给业界又增加一个负担。

	新建的第三级以上网络上线运行前应当委托网络安全等级测评机构按照网络安全等级保护有关标准规范进行等级测评，通过等级测评后方可投入运行。	当由被委托的网络安全等级测评机构进行。	
23	【等级测评】第三级以上网络的运营者应当每年开展一次网络安全等级测评，发现并整改安全风险隐患，并每年将开展网络安全等级测评的工作情况及测评结果向备案的公安机关报告。	建议明确每年一次的网络安全等级测评是由运营者自我测评还是由第三方测评，本条是否要求按照 GBR/T 28448 和 28449 标准对公司进行评价。	
25	【自查工作】网络运营者应当每年对本单位落实网络安全等级保护制度情况和网络安全状况至少开展一次自查，发现安全风险隐患及时整改，并向备案的公安机关报告。		此处的“网络”包括第一级网络。根据第十八条规定，只有二级以上网络才需要向公安机关备案。请明确，一级网络的运营机构是否也需要备案？
27	网络安全等级测评机构等网络服务提供者应当保守服务过程中知悉的国家秘密、个人信息和重要数据…	建议修改为： “网络安全等级测评机构等网络服务提供者应当保守服务过程中知悉的国家秘密、商业秘密、个人信息和重要数据…”	我们认为，商业秘密在此也应得到周密的保护。 此外，根据《网络安全法》给出的定义，“网络服务提供者”指的是网络运营者。而在本条例中，“网络服务提供者”还包括第三方机构如“网络安全等级测评机构”，为何会有这种变化，请给予解释。
28	【产品服务采购使用的安全要求】网络运营者应当采购、使用符合国家法律法规和有关标准规范要求的网络产品和服务。 第三级以上网络运营者应当采用与其安全保护等级相适应的网络产品和服务；对重要部位使用的网络产品，应当委托专业测评机构进行专项测试，根据测试结果选择符合要求的网络产	建议修改为： “【产品服务采购使用的安全要求】网络运营者应当采购、使用符合国家法律法规和有关标准规范要求的网络产品和服务。 第三级以上网络运营者应当采用与其安全保护等级相适应的网络产品和服务~~；对重要部位使用的网络产品，应当委托专业测评机构进行专~~	希望进一步明确 “符合要求的网络产品”以及“重要部位”的具体含义。这些短语含义模糊，有可能被用于支持对某些产品给予优惠待遇。本条例应避免使其条款为违反《关贸总协定》（GATT）、《服务贸易总协定》（GATS）和 TBT 协议中的重要义务创造便利。参见 GATT 第 III 条第 4 项，GATS 第十七条，以及 TBT 协议第 2 条。 在此我们想指出，根据《网络安全法》第三十五条，关键信息基础设施的运营者“采购网络产品和服务，可能影响国家安全的，应当通过国家安全审查。”我们认为，三级网络运营者并不等同于关键信息基础设施运营者，因此建议这条规定，避免行政权力被滥用，也避免对中国创新造成伤害。

	品；采购网络产品和服务，可能影响国家安全的，应当通过国家网信部门会同国务院有关部门组织的国家安全审查。	~~项测试，根据测试结果选择符合要求的网络产品；采购网络产品和服务，可能影响国家安全的，应当通过国家网信部门会同国务院有关部门组织的国家安全审查~~。”	最后，本条似乎对购买某些网络产品和服务的三级以上网络运营者提出了新的测试要求。这个新的认证和测评制度与已有的制度重复，无助于加强网络安全，只能给市场带来更多不确定性。
29	【技术维护要求】第三级以上网络应当在境内实施技术维护，不得境外远程技术维护。因业务需要，确需进行境外远程技术维护的，应当进行网络安全评估，并采取风险管控措施。实施技术维护，应当记录并留存技术维护日志，并在公安机关检查时如实提供。	建议修改为： “【技术维护要求】被认定为关键信息基础设施的第三级以上网络应当~~在境内~~实施技术维护~~，不得境外远程技术维护。因业务需要，确需进行境外远程技术维护的，应当进行网络安全评估，并采取风险管控措施~~。实施技术维护，应当记录并留存技术维护日志，并在公安机关检查时如实提供。”	由于三级网络运营不等同于关键信息基础设施运营者，我们建议增加一个限定性短语“被认定为关键信息基础设施的”，使表述更准确，避免行政权力的不适当扩展，同时也避免对中国创新造成伤害。 我们还建议删除“只能在境内实施技术维护”的要求，否则将给国际厂商带来沉重的负担，可能会限制能够提供给网络运营者的产品范围。如果该技术维护要求确需保留，其范围必须限定，必须规定哪些企业需要进行“网络安全评估”以及在境外远程维护情况下所使用的方法。
31	【数据和信息安全保护】网络运营者应当建立并落实重要数据和个人信息安全保护制度；采取保护措施，保障数据和信息在收集、存储、传输、使用、提供、销毁过程中的安全；建立异地备份恢复等技术措施，保障重要数据的完整性、保密性和可用性。	建议缩小第三十一条的范围，与《网络安全法》第三十七条保持一致 此外，建议删除“异地”一词，与《网络安全法》保持一致。	本条例草案的数据规定过于宽泛，远超《网络安全法》规定的内容，表述也不明确。例如，我们不清楚哪些数据构成条例草案所说的“重要数据”。此外，条例草案似乎适用于一般意义上的网络运营者，而不是只适用于关键信息基础设施的运营者。《网络安全法》第三十七条给出了更加明确的限定，规定“关键信息基础设施的运营者应在中国人民共和国境内存储个人信息和重要业务数据。” 其次，根据《网络安全法》第二十一条和第三十四条，关键信息基础设施运营者应对重要系统和数据进行容灾备份（异地备份）。网络运营者则应“采取数据分类、重要数据备份和加密等措施。”
33	【审计审核要求】网络运营者建设、运营、维护和使用网络，向社会公众提供需取得行政许可的经营活动的，相关主管部门应当将网络安全等级保护制度落实情况纳入审计、审核范围。	建议删除本条。	强化各行业监管机构的审计、审核权力将加深业界对保密性的担忧，并且还将造成公安部和其他部门执行标准不一，重复监管。

34	【新技术新应用风险管控】网络运营者应当按照网络安全等级保护制度要求，采取措施，管控云计算、大数据、人工智能、物联网、工控系统和移动互联网等新技术、新应用带来的安全风险，消除安全隐患。	我们强烈建议删除有关云计算、大数据、人工智能、物联网、工控系统和移动互联网等商用行业的内容。在本条例中，监管部门规定了一系列影响重大且繁琐的网络安全保护程序，其结果是将会极大增加运营者成本，阻碍中国正在快速增长的技术行业的成长，而且对网络安全不会起到任何促进作用。事实上，更为有效的方法是集中针对真正重要的涉及国家安全的网络进行监管，比如军事网络和政务网络。 此外，建议对“新技术”一词进行更精确地定义。	本条例草案第三十四条把安全等级保护制度的适用范围扩展到了商业领域。由于企业的资源、员工数量和数据量都很有限，实施等级保护制度有可能给企业带来巨大的运营障碍。例如，很多新的技术公司都拥有工业控制系统网络，这是否使其自动成为三级网络运营者？
45	【确定密码要求】国家密码管理部门根据网络的安全保护等级、涉密网络的密级和保护等级，确定密码的配备、使用、管理和应用安全性评估要求，制定网络安全等级保护密码标准规范。		希望明确说明“**安全性评估要求**”何时确定，“**网络安全等级保护密码标准规范**”何时制定。USITO 希望，如果现有法规规章已包含对密码的测评要求，拟制定的新规应避免提出同样的测评要求。 此外，建议明确第 5 章“密码管理”所针对的是 1）以密码技术为核心功能的产品，还是 2）所有含有密码技术的产品。我们建议应当遵循国家密码管理委员会办公室在 2000 年发布的说明，[3] 即本条例只适用于以加密解密操作为核心功能的产品。
46	【涉密网络密码保护】涉密网络及传输的国家秘密信息，应当依法采用密码保护。 密码产品应当经过密码管理部门批准，采用密码技术的软件系统、硬件设备等产品，应当通过密码检测。	【涉密网络密码保护】涉密网络及传输的国家秘密信息，应当依法采用密码保护。 密码产品应当经过密码管理部门批准~~，采用密码技术的软件系统、硬件设备等产品，应当通过密码检测~~。	在现代信息技术时代，几乎所有产品都使用密码技术。对于使用密码技术但不属于国家密码管理部门规定的“密码产品”一类的产品，如果要求其必须通过密码检测（可能需要中国密码方式），就会存在一个风险：即很多产品，尤其是跨国公司生产的硬件和软件产品，就会因此而被排除在中国境内涉密网络之外。这将对全球贸易产生不利影响。此外，把含有密码技术的产品排除在涉密网络之外，还将妨碍系统互联互通，实现全球联通。

[3] 中华人民共和国国家密码管理委员会办公室在 2000 年 3 月发布的关于商用密码管理有关问题的说明中表示，“纳入本条例管理范围的‘密码产品及含有密码技术的设备’，只限于以加密解密操作为核心功能的专用硬件、软件，其他如无线手机、Windows 软件、浏览器软件等都不在这个范围之内。”

	密码的检测、装备、采购和使用等，由密码管理部门统一管理；系统设计、运行维护、日常管理和密码评估，应当按照国家密码管理相关法规和标准执行。	密码的检测、装备、采购和使用等，由密码管理部门统一管理；系统设计、运行维护、日常管理和密码评估，应当按照国家密码管理相关法规~~和标准~~执行。	中国作为世界半导体理事会（WSC）政府与政府间半导体会议（GAMS）的积极参与者，承诺遵守 WSC 关于大众化 ICT 产品商用密码技术的密码方面的原则，其中包括限制对商用密码进行监管，并禁止指定使用某一加密技术。这样也确保符合中国加入世界贸易组织（WTO）时做出的承诺，遵守 《关贸总协定》、《服务贸易总协定》和《技术贸易壁垒协定》（参阅 GATT 第三条第 4 项，GATS 第十七条，和 TBT 协议第二条；TBT 协议第二条规定："各成员应保证技术法规的制定、采用或实施在目的或效果上均不对国际贸易造成不必要的障碍。"）(https://www.wto.org/english/docs_e/legal_e/17-tbt_e.htm).
47	【非涉密网络密码保护】非涉密网络应当按照国家密码管理法律法规和标准的要求，使用密码技术、产品和服务。第三级以上网络应当采用密码保护，并使用国家密码管理部门认可的密码技术、产品和服务。 第三级以上网络运营者应在网络规划、建设和运行阶段，按照密码应用安全性评估管理办法和相关标准，委托密码应用安全性测评机构开展密码应用安全性评估。网络通过评估后，方可上线运行，并在投入运行后，每年至少组织一次评估。密码应用安全性评估结果应当报受理备案的公安机关和所在地设区市的密码管理部门备案。	建议删除本条规定。随着等级保护制度扩展到政府网络和商务网络，本条规定意味着密码技术在商用网络部署之前应得到国家批准。这一规定无谓地限制了非政府和商业机构对网络安全产品和服务的使用。由于网络安全领域是动态的，且在不断变化之中，一个风险是，企业可能无法及时获得最先进的或最新发布的产品，因为政府部门还没有签发批文。 此外，我们建议，在网络投入运行后，只有在网络发生重大变化时才需要开展评估。	我们希望了解在三级以上网络使用密码产品和服务的规定。目前跨国公司生产的大多数产品和服务只使用国际公认的密码加密技术，不支持中国加密方式。这将把大多数跨国公司产品排除在三级网络之外，严重损害全球信息技术贸易。这些条款将违背上述 47 条意见中阐述的 WSC/GAMS 原则，以及 WTO/TBT 原则。 其次，在三级以上网络上只允许使用国家密码管理部门认可的密码技术、产品和服务还将妨碍和影响用户（包括商业公司）实现全球联通。再次，对密码技术的管理过于颗粒化，缺乏灵活度。 最后一点，"每年至少组织一次密码评估"似缺乏必要性，将会给企业带来沉重的负担。
50	【安全检查】公安机关对第三级以上网络运营者每年至少开展一次安全检查。涉及相关行业的可以会同其行业主管部门开展安全检查。必要时，公安机关可以委托社会力量提供技术支持。	建议修改如下： "【安全检查】公安机关对第三级以上网络运营者每年至少开展一次安全检查。涉及相关行业的可以会同其行业主管部门开展安全检查。必要时，公安机关可以委	希望进一步说明哪些机构构成"社会力量"。 本条还表明，政府有可能委托第三方开展侵入式的安全监测，这将引发业界对知识产权潜在泄露的担忧。

	公安机关依法实施监督检查，网络运营者应当协助、配合，并按照公安机关要求如实提供相关数据信息。	托~~社会力量~~有资质的安全检查机构提供技术支持。 公安机关依法实施监督检查，并提前足够时间以书面方式通知检查内容、参加人员及将采取的行动，网络运营者应当协助、配合，并按照公安机关要求如实提供相关数据信息。”	
55	【事件调查】公安机关应当根据有关规定处置网络安全事件，开展事件调查，认定事件责任，依法查处危害网络安全的违法犯罪活动。必要时，可以责令网络运营者采取阻断信息传输、暂停网络运行、备份相关数据等紧急措施。 网络运营者应当配合、支持公安机关和有关部门开展事件调查和处置工作。	建议删除本条最后一句。如果确需保留，建议修改如下： “网络运营者应当依法配合、支持公安机关和有关部门开展事件调查和处置工作。”	鉴于第一款中已规定，“公安机关可以责令网络运营者采取阻断信息传输、暂停网络运行、备份相关数据等紧急措施”，因此本条最后一句属于重复。
56	【紧急情况断网措施】网络存在的安全风险隐患严重威胁国家安全、社会秩序和公共利益的，紧急情况下公安机关可以责令其停止联网、停机整顿。	【紧急情况断网措施】网络存在的安全风险隐患严重威胁国家安全、社会秩序和公共利益的，紧急情况下公安机关可以经国务院决定或批准，责令其停止联网、停机整顿。	根据《网络安全法》第五十八条，因处置重大突发社会安全事件的需要，经国务院决定或者批准，可以在特定区域对网络通信采取限制等临时措施。
59	【行业监督管理】		本条需要进一步明确。监督管理涉及哪些内容？
62	【网络安全约谈制度】省级以上人民政府公安部门、保密行政管理部门、密码管理部门在履行网络安全等级保护监督管理职责中，发现网络存在较大安全风险隐患或者发生安全事件的，可以约谈网络运营	【网络安全约谈制度】省级以上人民政府公安部门、保密行政管理部门、密码管理部门在履行网络安全等级保护监督管理职责中，发现网络存在较大安全风险隐患或者发生安全事件的，可以约谈网络运营	

	者的法定代表人、主要负责人及其行业主管部门。	者的法定代表人、主要负责人及其行业主管部门。在约谈之前，相关部门应事先书面通知被约谈方。	
66	【网络安全服务责任】违反本条例第二十六条第三款，第二十七条第二款规定的，由公安机关责令改正，可以根据情节单处或者并处警告、没收违法所得、处违法所得一倍以上十倍以下罚款，没有违法所得的，处一百万元以下罚款。	【网络安全服务责任】违反本条例第二十六条第三二款，第二十七条第二款规定的，由公安机关责令改正，可以根据情节单处或者并处警告、没收违法所得、处违法所得一倍以上十倍以下罚款，没有违法所得的，处一百万元以下罚款	
73	【生效时间】本条例由自　年　月　日起施行。	【生效时间】本条例自　年　月　日起施行。自生效之日起，《信息系统等级保护管理办法》（2007年发布）同时自动废止。	