海问观察：数据合规专题——《网络安全审查办法（征求意见稿）》评析

傅鹏、赵卿梦

2019 年 5 月 24 日，国家互联网信息办公室发布了《网络安全审查办法（征求意见稿）》（以下简称“新办法”），面向社会公开征求意见，相较于 2017 年发布的《网络产品和服务安全审查办法（试行）》（以下简称“原办法”），新办法对安全审查启动、安全审查需要提供的资料、安全审查程序及安全审查内容等方面做出了修改和完善。其中，特别对整个安全审查流程，包括安全审查期限、各参与机构职责划分做出了具体的规定。

本文试图通过新办法与原办法的条文对比分析形式，就新办法对网络产品和服务的安全审查制度的修改和完善进行介绍与评析。

	《网络产品和服务安全审查办法（试行）》	《网络安全审查办法（征求意见稿）》	比较评析
制定目的	**第一条** 为提高网络产品和服务安全可控水平，防范网络安全风险，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》等法律法规，制定本办法。	**第一条** 为提高关键信息基础设施安全可控水平，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》等法律法规，制定本办法。 **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，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。法律、行政法规另有规定的，依照其规定。 **第十八条第二款** 安全可控是指产品和服务提供者不得利用提供产品和服务的便利条	（1）新办法所述“影响或可能影响国家安全”具体判断标准，可使用新办法第六条运营者自主申报的四个情况（详见下文）作为参考。其中，“大量个人信息和重要数据”的判断标准有待进一步明确；现阶段已经公布的《个人信息和重要数据出境安全评估办法（征求意见稿）》中相关的规定具有相近的背景，即“（一）含有或累计含有 50 万人以上的个人信息；（二）数据量超过

	《网络产品和服务安全审查办法（试行）》	《网络安全审查办法（征求意见稿）》	比较评析
		件非法获取用户数据、非法控制和操纵用户设备，不得利用用户对产品和服务的依赖性牟取不正当利益或者迫使用户更新换代等。	1000GB”，但最终采取什么标准还需拭目以待。
审查对象	**第二条** 关系国家安全的网络和信息系统采购的重要网络产品和服务，应当经过网络安全审查。 **第十条** 公共通信和信息服务、能源、交通、水利、金融、公共服务、电子政务等重要行业和领域，以及其他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，应当通过网络安全审查。产品和服务是否影响国家安全由关键信息基础设施保护工作部门确定。	**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，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。法律、行政法规另有规定的，依照其规定。 **第十八条** 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。 **第十九条** 网络安全审查工作机制成员单位认为影响或可能影响国家安全的网络产品和服务采购活动、信息技术服务活动，网络安全审查办公室按程序报中央网络安全和信息化委员会批准，依照本办法进行审查。	（1）原办法中对审查对象的范围划定在公共通信和信息服务、能源等“重要行业和领域”以及“其他关键信息基础设施的运营者”，但就法规中列举的“重要行业和领域”是否属于“关键信息基础设施的运营者”的范围内还是与“关键信息基础设施的运营者”为并列关系，现有规定对此没有予以特别明确的说明。相比而言，新办法从文义来看，删去了与“重要行业和领域”相关的范围，明确了“关键信息基础设施的运营者”在一定条件

	《网络产品和服务安全审查办法（试行）》	《网络安全审查办法（征求意见稿）》	比较评析
	审查对象范围： （1）重要行业和领域运营者采购网络产品和服务； （2）关键信息基础设施的运营者采购网络产品和服务。 **确定标准：** 关系国家安全，是否影响国家安全由关键信息基础设施保护工作部门确定。	**审查对象范围：** 关键信息基础设施运营者采购网络产品和服务，运营者的范围由关键信息基础设施保护工作部门认定。 **确定标准：** 影响或可能影响国家安全的。	下应当申报安全审查的要求，使得规定本身更加明确，在关键信息基础设施的识别问题明确之后将较大地增加这一规定的适用性和明确性； （2）尽管明确了“关键信息基础设施的运营者”在一定条件下是安全审查的申报主体，但是，根据新办法第十九条规定，成员单位认定为影响或可能影响国家安全的网络产品和服务采购活动、信息技术服务活动经批准后也需按照新办法进行安全审查。可见，安全审查对象不仅限于关键信息基础设施运营者采购网络产品和服务的情形，主管机关可以依据新办法以及其他配套规定对关键信息基础设施运营者以外的主体的有关行为进行安全审查； （3）就关键信息基础设施运营者具体的范围，新办法明确

	《网络产品和服务安全审查办法（试行）》	《网络安全审查办法（征求意见稿）》	比较评析
			由关键信息基础设施保护工作部门认定。目前已经生效的法律法规对于关键信息基础设施范围仍不明确，参照《关键信息基础设施安全保护条例（征求意见稿）》，关键信息基础设施保护范围包括： • 政府机关和能源、金融、交通、水利、卫生医疗、教育、社保、环境保护、公用事业等行业领域的单位； • 电信网、广播电视网、互联网等信息网络，以及提供云计算、大数据和其他大型公共信息网络服务的单位； • 国防科工、大型装备、化工、食品药品等行业领域科研生产单位； • 广播电台、电视台、通讯社等新闻单位； • 其他重点单位。 此外，根据《关于开展关键信息基础设施网络安全检查的通知》（中网办发〔2016〕3 号）

	《网络产品和服务安全审查办法（试行）》	《网络安全审查办法（征求意见稿）》	比较评析
			中《网络安全检查操作指南》规定，认定关键信息基础设施通常包括三个步骤，一是确定关键业务，二是确定支撑关键业务的信息系统或工业控制系统，三是根据关键业务对信息系统或工业控制系统的依赖程度，以及信息系统发生网络安全事件后可能造成的损失认定关键信息基础设施。但该通知发布在《中华人民共和国网络安全法》（“《网络安全法》”）之前，该等认定标准是否会被主管机关采纳并应用于此后的关键信息基础设施识别的标准性文件中仍具有不确定性。
审查的启动	**第八条** 网络安全审查办公室按照国家有关要求、根据全国性行业协会建议和用户反映等，按程序确定审查对象，组织第三方机构、专家委员会对网络产品和服务进行网络安全审查，并发布或在一定范围内通报审查结果。	**第六条** 运营者采购网络产品和服务时，应预判产品和服务上线运行后带来的潜在安全风险，形成安全风险报告。可能导致以下情况的，应当向网络安全审查办公室申报网络安全审查： （一）关键信息基础设施整体停止运转或主要功能不能正常运行； （二）大量个人信息和重要数据泄露、丢失、毁损或出境；	（1）主管机关依职权启动安全审查是原办法中安全审查启动的主要方式，新办法中将依运营者申请作为启动安全审查的主要方式； （2）新办法第六条中“运营者”直接指向关键信息基础设施运营者，而第十九条未对审

	《网络产品和服务安全审查办法（试行）》	《网络安全审查办法（征求意见稿）》	比较评析
		（三）关键信息基础设施运行维护、技术支持、升级更新换代面临供应链安全威胁； （四）其他严重危害关键信息基础设施安全的风险隐患。 **第十九条** 网络安全审查工作机制成员单位认为影响或可能影响国家安全的网络产品和服务采购活动、信息技术服务活动，网络安全审查办公室按程序报中央网络安全和信息化委员会批准，依照本办法进行审查。	查对象设置限定范围，因此，从目前新办法的条文看来，依网络运营者申请启动的安全审查对象仅限于关键信息基础设施运营者。
	依职权启动： 网络安全审查办公室依职权启动安全审查。	**（1）依申请启动** 运营者自主判断后，申请启动安全审查； **（2）依职权启动** 网络安全审查办公室报中央网络安全和信息化委员会批准，启动安全审查。	
审查机构	**第五条** 国家互联网信息办公室会同有关部门成立网络安全审查委员会，负责审议网络安全审查的重要政策，统一组织网络安全审查工作，协调网络安全审查相关重要问题。 网络安全审查办公室具体组织实施网络安全审查。 **第六条** 网络安全审查委员会聘请相关专家组成网络安全审查专家委员会，在第三	**第四条** 中央网络安全和信息化委员会统一领导网络安全审查工作。 **第五条** 国家互联网信息办公室会同国家发展和改革委员会、工业和信息化部、公安部、国家安全部、商务部、财政部、中国人民银行、国家市场监督管理总局、国家广播电视总局、国家保密局、国家密码管理局建立国家网络安全审查工作机制。网络安全审查办公室设在国家互联网信息办公室，负责组织	新办法相较于原办法： （1）明确中央网络安全和信息化委员会对安全审查工作的领导地位； （2）将原办法中“网络安全审查委员会”的具体成员予以明确；

	《网络产品和服务安全审查办法（试行）》	《网络安全审查办法（征求意见稿）》	比较评析
	方评价基础上，对网络产品和服务的安全风险及其提供者的安全可信状况进行综合评估。 **第八条** 网络安全审查办公室按照国家有关要求、根据全国性行业协会建议和用户反映等，按程序确定审查对象，组织第三方机构、专家委员会对网络产品和服务进行网络安全审查，并发布或在一定范围内通报审查结果。 **第九条** 金融、电信、能源、交通等重点行业和领域主管部门，根据国家网络安全审查工作要求，组织开展本行业、本领域网络产品和服务安全审查工作。	制定网络安全审查相关制度规定和工作程序、组织网络安全审查、监督审查决定的实施。	（3）新办法中未体现第三方评估及专家评估是否作为安全审查的必要环节，而仅在特别审查程序中要求网络安全审查办公室听取专业机构和专家意见； （4）重点行业和领域的安全审查不再与关键信息基础设施运营者的安全审查制度予以区分。但是这是否意味着重点行业和领域的运营者采购网络产品和服务不再需要进行安全审查，还有待主管部门对关键信息基础设施运营者的具体涵盖范围进行明确。
	（1）政策审议及组织、协调机构： 网络安全审查委员会（国家互联网信息办公室会同有关部门） **（2）安全评估机构** 第三方机构及安全审查专家委员会 **（3）具体实施机构** 网络安全审查办公室组织第三方机构、专家委员会审查 **（4）重点行业和领域的审查机构** 金融、电信、能源、交通等重点行业和领	**（1）组织、领导机构** 中央网络安全和信息化委员会 **（2）具体实施机构** 网络安全审查办公室 **（3）成员单位** 国家互联网信息办公室会同国家发展和改革委员会、工业和信息化部、公安部、国家安全部、商务部、财政部、中国人民银行、国家市场监督管理总局、国家广播电视总局、国家保密局、国家密码管理局建立国家	

	《网络产品和服务安全审查办法（试行）》	《网络安全审查办法（征求意见稿）》	比较评析
	域主管部门，组织开展本行业、本领域网络产品和服务安全审查工作	网络安全审查工作机制 **（4）相关部门、专业机构、专家** 进入特别程序的安全审查，还应听取相关部门、专业机构、专家的意见	
审查程序	**第三条** 坚持企业承诺与社会监督相结合，第三方评价与政府持续监管相结合，实验室检测、现场检查、在线监测、背景调查相结合，对网络产品和服务及其供应链进行网络安全审查。	**第九条** 网络安全审查办公室受理网络安全审查后，应在30个工作日内完成初步审查，情况复杂的可延长15个工作日。 **第十一条** 网络安全审查办公室完成初步审查后，应形成审查结论建议，并送网络安全审查工作机制成员单位征求意见。审查结论建议包括通过审查、附条件通过审查、未通过审查三种情况。 网络安全审查工作机制成员单位应在15个工作日内书面回复意见。网络安全审查工作机制成员单位意见一致的，网络安全审查办公室以书面形式将审查结论反馈运营者；意见不一致的，进入特别审查程序并通知运营者。 **第十二条** 进入特别审查程序的，网络安全审查办公室应进一步听取相关部门、专业机构、专家意见，进行深入分析评估，形成审查结论建议，征求网络安全审查工作机制成员单位意见后，按程序报中央网络安全和信	（1）原办法强调第三方评价与政府持续监管相结合，方式上强调检测、检查、监测与调查等方面，但未对安全审查的具体程序作出明确规定； （2）新办法细化了安全审查的程序，按照新办法，安全审查从受理到审查结束最慢需要45个工作日，情况复杂的最慢可至125个工作日或更久。

	《网络产品和服务安全审查办法（试行）》	《网络安全审查办法（征求意见稿）》	比较评析
		息化委员会批准。 **第十三条** 特别审查原则上应在 45 个工作日内完成，情况复杂的可以延长。 **第十六条** 运营者加强安全管理，督促产品和服务提供者认真履行网络安全审查中作出的承诺。 网络安全审查办公室通过抽查、接受举报等形式加强事中事后监管。	
	无具体规定	**明确了安全审查的具体程序：** **（1）受理** **（2）初步审查 30+15** 30 个工作日内完成，情况复杂可延长 15 个工作日 **（3）征求意见 15** 初步审查形成的审查结论建议应当送成员单位征求意见，成员单位应在 15 个工作日内回复 **（4）特别审查程序 45+N** 成员单位意见不一致的，启动特别审查程序，特别审查程序应在 45 个工作日内完成，情况复杂的可以延长	
申报材料	无具体规定	**第八条** 运营者申报网络安全审查时，应当	新办法对安全审查需要申报

	《网络产品和服务安全审查办法（试行）》	《网络安全审查办法（征求意见稿）》	比较评析
		提交以下材料： （一）申报书； （二）本办法第六条中的安全风险报告； （三）采购合同、协议等； （四）网络安全审查办公室要求的其他材料。	的材料作出了相对具体的规定。
审查内容	**第四条** 网络安全审查重点审查网络产品和服务的安全性、可控性，主要包括： （一）产品和服务自身的安全风险，以及被非法控制、干扰和中断运行的风险； （二）产品及关键部件生产、测试、交付、技术支持过程中的供应链安全风险； （三）产品和服务提供者利用提供产品和服务的便利条件非法收集、存储、处理、使用用户相关信息的风险； （四）产品和服务提供者利用用户对产品和服务的依赖，损害网络安全和用户利益的风险； （五）其他可能危害国家安全的风险。	**第十条** 网络安全审查重点评估采购活动可能带来的国家安全风险，主要考虑以下因素： （一）对关键信息基础设施持续安全稳定运行的影响，包括关键信息基础设施被控制、被干扰和业务连续性被损害的可能性； （二）导致大量个人信息和重要数据泄露、丢失、毁损、出境等的可能性； （三）产品和服务的可控性、透明性以及供应链安全，包括因为政治、外交、贸易等非技术因素导致产品和服务供应中断的可能性； （四）对国防军工、关键信息基础设施相关技术和产业的影响； （五）产品和服务提供者遵守国家法律与行政法规情况，以及承诺承担的责任和义务； （六）产品和服务提供者受外国政府资助、控制等情况； （七）其他可能危害关键信息基础设施安全	（1）对持续稳定运营的要求更高，不再要求被“非法”控制，仅有被控制的可能性也需纳入审查因素；同时“中断运行”被替换为“业务连续性被损害”也体现出对设施运行的更高要求； （2）对个人信息和重要数据的保护，原办法侧重提供者的“合法性”，新办法则一定程度上提高了要求，不仅审查合法性，还要求提供者应避免信息泄露、丢失、毁损、出境的可能性； （3）增加了对国防军工等相关技术和产业影响的审查因素；

	《网络产品和服务安全审查办法（试行）》	《网络安全审查办法（征求意见稿）》	比较评析
		和国家安全的因素。	（4）对提供者的主体审查更加宽泛； （5）增加与境外相关的审查，包括数据的跨境以及提供者与外国政府的关联的审查； （6）除国家安全外，增加了对关键信息基础设施安全的审查要素。
提供者的配合义务	无具体规定	**第七条** 对于申报网络安全审查的采购活动，运营者应通过采购文件、合同或其他有约束力的手段要求产品和服务提供者配合网络安全审查，并与产品和服务提供者约定网络安全审查通过后合同方可生效。	增加了网络产品和服务提供者的配合审查义务，但是对违反此等义务并未设置具体的惩罚措施。同时，明确了采购合同应当约定在网络安全审查通过后方可生效。 但是，根据《中华人民共和国合同法》的规定，依法成立的合同，自成立时生效；法律、行政法规规定应当办理批准、登记等手续生效的，依照其规定。原办法和新办法都是国家互联网信息办公室颁布的规

	《网络产品和服务安全审查办法（试行）》	《网络安全审查办法（征求意见稿）》	比较评析
			章制度，并不严格属于《中华人民共和国立法法》规定的行政法规，因此，如果合同双方未约定网络安全审查通过后合同方可生效，则合同在签署成立后已经生效。对于本条规定的具体解释及落实情况，有待正式稿或实践执法过程中进一步观察。
法律后果	**第十五条** 违反本办法规定的，依照有关法律法规予以处理。	**第十七条** 运营者违反本办法规定的，依照《中华人民共和国网络安全法》第六十五条的规定处理。	原办法规定较为模糊，新办法具体指向了《网络安全法》第六十五条规定的罚则。

相较于《网络产品和服务安全审查办法（试行）》，《网络安全审查办法（征求意见稿）》对网络产品和服务的安全审查制度的规定进行了细化和完善，特别是对安全审查的具体流程做出了明确规定。但是，对于安全审查制度中安全审查适用对象的具体细化分类以及针对每一项义务之违反的具体惩罚措施等方面还有待相关细则、指南的出台以及实践中施行的检验。

海问代表客户进行了大量与人工智能、大数据及泛科技相关的投融资项目，在该等项目中海问提供了以数据合规问题作为关注要点的专项尽职调查服务，并在此过程中积累了业务导向的、针对数据合规问题的解决方案经验。同时，海问长期以来也为互联网公司及跨国企业提供日常数据合规咨询服务。海问将基于对该领域的理解和实践经验，对网络安全审查制度及其后续配套实施细则、措施的落地、执行予以持续关注。