汉坤法律评述

2022 年 1 月 4 日

HANKUN
汉 坤 律 师 事 务 所
Han Kun Law Offices

北京 | 上海 | 深圳 | 香港

快评新《网络安全审查办法》

作者：段志超 | 蔡克蒙 | 胡敏喆

2022 年 1 月 4 日，国家互联网信息办公室（简称**“网信办”**）、中国证券监督管理委员会等十三部委正式联合出台了修订后的《网络安全审查办法》（**“新《审查办法》”**），标志着业界关注已久的修改后的网络安全审查制度在新年伊始正式出台。新《审查办法》将于 2022 年 2 月 15 日正式实施。新的审查办法基本沿袭了此前 13 部委在 2021 年 7 月 10 日发布的*《网络安全审查办法》（修订草案征求意见稿）*（**“征求意见稿”**）所提出的制度框架，并在征求意见稿基础上做出了几处关键修订，本文将对这些修订进行简要解读。同时随附**新《审查办法》与征求意见稿的对比，供读者参考。**

一、沿用“国外上市”概念，可能旨在排除赴香港上市的运营者主动申报网络安全审查的义务

新《审查办法》仍沿用了征求意见稿中“国外上市”的概念，并未对其进行进一步界定。但从《网络数据安全管理条例》（征求意见稿）区分“赴香港上市”和“国外上市”网络安全审查申报标准之后，又在新《审查办法》将主动申报义务限定在“国外上市”来看，新《审查办法》应旨在免除赴香港上市的运营者主动申报网络安全审查的义务，但这一理解仍有待通过监管机构的后续实践加以验证。此外，由于新《审查办法》与此前审查办法及征求意见稿均赋予了监管机构主动依职权开展网络安全审查的权力，因此不排除在实践中部分赴香港上市企业如涉及大量敏感数据处理活动时，出于谨慎考虑主动申报网络安全。

与此前征求意见稿相同，新《审查办法》并未对受审查的上市方式进行限定，只是在申报材料中将需申报的材料更严谨的界定为“首次公开募股（IPO）等上市申请文件”。我们仍然认为除 IPO（首次公开募集股份并上市）外，中概股公司在美国上市可能采取的 SPAC（特殊目的收购公司）并购、RTO（反向兼并/借壳上市）、Direct Listing（直接上市）等方式均应主动申请申报网络安全审查。

二、赴国外上市需申报网络安全审查的主体改为“网络平台运营者”

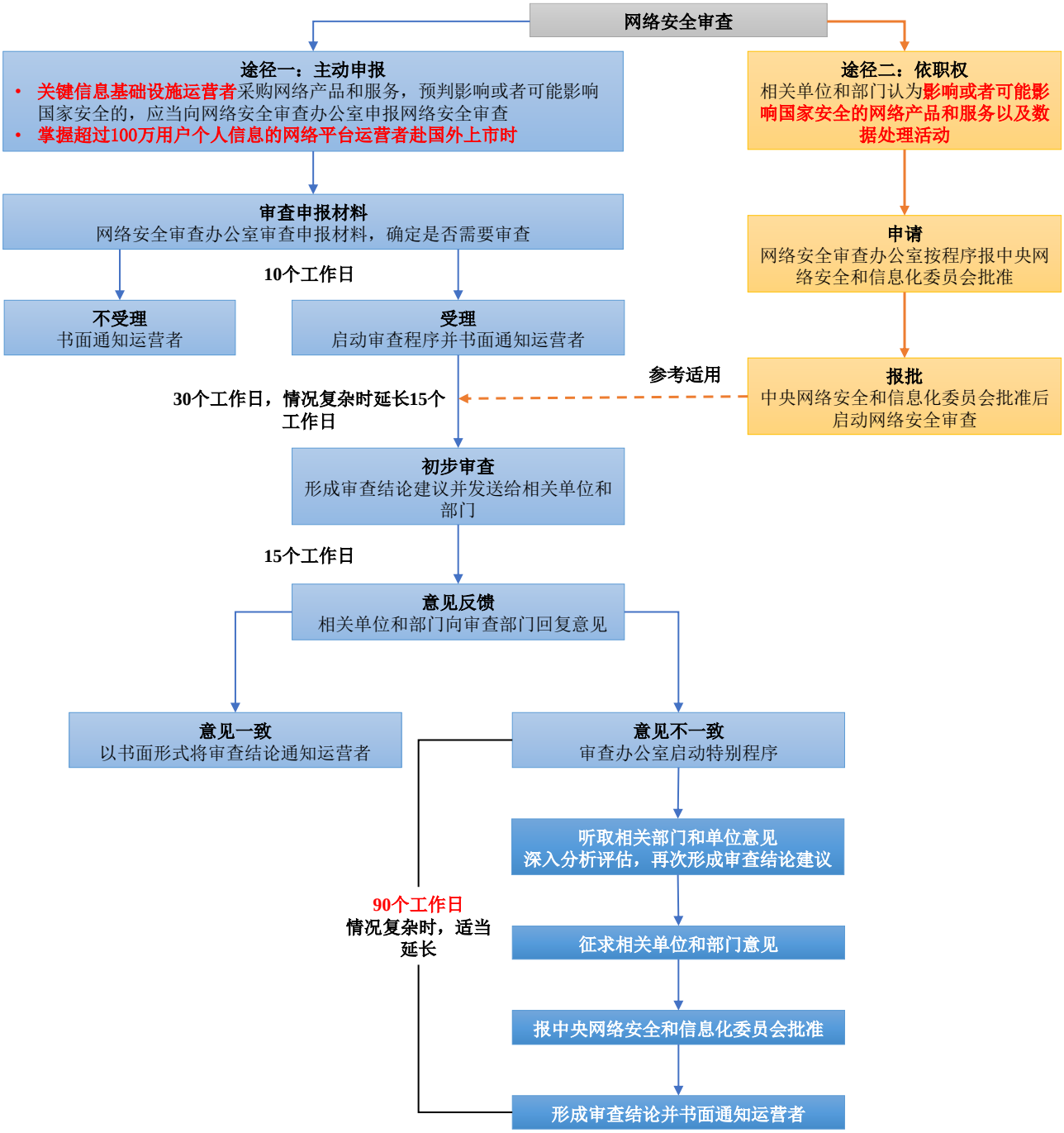
新《审查办法》规定“掌握超过 100 万用户个人信息的网络平台运营者赴国外上市，必须向网络安全审查办公室申报网络安全审查。”这一规定仍沿袭了此前征求意见稿对需开展申报的上市地及用户数量标准的界定，但将申请主体由此前的“数据处理者”改为“网络平台运营者”。新《审查办法》本身未对“网络平台运营者”的概念进行界定。网信办此前公布的《网络数据安全管理条例》（征求意见稿）曾将“互联网平台运营者”界定为“为用户提供信息发布、社交、交易、支付、视听等互联网平台服务的数据处理者”。按通常理解，“网络平台运营者”的范围应小于此前的“数据处理者”，似不包含不提供线上平台服务的各类消费品公司的自营电商服务。但由于“网络平台运营者”这一概念较为模糊，监管机关在实践中仍有较大的解释空间要求“掌握超过 100 万用户个人信息”的各类运营者均需主动申报网络安全审查。

三、申报网络安全审查的时间点及结果

根据新《审查办法》答记者问，网络平台运营者应在向国外证券监管机构提出上市申请之前，申报网络安全审查。申报的结果可能包括，一是无需审查；二是启动审查后，经研判不影响国家安全的，可继续赴国外上市程序；三是启动审查后，经研判影响国家安全的，不允许赴国外上市。在前两种情况下，运营者可以继续向国外证券监管机构提出上市申请，但根据此前证监会发布的《境内企业境外发行证券和上市备案管理办法》（征求意见稿），企业需要在上市申请提交后三个工作日向证监会履行备案手续。

四、特别审查程序的时限进一步延长

新《审查办法》的审查流程总体沿用了现行审查办法及征求意见稿的流程，只是将在出现网络安全审查工作机制成员单位、相关部门意见不一致情况下，需征求有关部门意见并报中央网络安全和信息化委员会批准的特别审查流程期限由征求意见稿规定的 3 个月进一步延长至 **90 个工作日**，且情况复杂的仍可以延长。按照新《审查办法》，审查流程总体如下图所示。



五、审查期间应按要求采取预防和消减风险措施

新《审查办法》第 16 条新增规定“为了防范风险，当事人应当在审查期间按照网络安全审查要求采取预防和消减风险的措施。”从此前实践来看，“预防和消减风险的措施”可能包括暂停新用户注册、暂停 APP 下载等，还可能包括剥离相关数据资产甚至暂停相关网络产品服务等。

六、同步公布审查申请机制，正式开启审查窗口

值得注意的是，在新《审查办法》出台同时，网信办在答记者问上正式公布了审查申报和受理的途径，明确“网络安全审查办公室设在国家互联网信息办公室，具体工作委托中国网络安全审查技术与认证中心承担。中国网络安全审查技术与认证中心在网络安全审查办公室的指导下，承担接收申报材料、对申报材料

进行形式审查等任务。中国网络安全审查技术与认证中心设立网络安全审查咨询窗口。”我们也期待网络安全审查办公室及中国网络安全审查技术与认证中心后续尽快出台更明确的申报指南，为企业履行申报义务提供更加明确的指引。

《网络安全审查办法》修改前后对照表（与修订草案征求意见稿对比）

网络安全审查办法 （修订草案征求意见稿）	网络安全审查办法 ~~（修订草案征求意见稿）~~
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。	**第一条** 为了确保关键信息基础设施供应链安全，保障网络安全和数据安全，维护国家安全，~~依~~根据《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》、《关键信息基础设施安全保护条例》，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，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。	**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~~网络平台运营者~~）~~开展数据处理活动，影响或者可能影响国家安全的，应当按照本办法进行网络安全审查。 前款规定的关键信息基础设施运营者、网络平台运营者统称为当事人。
第三条 网络安全审查坚持防范网络安全风险与促进先进技术应用相结合、过程公正透明与知识产权保护相结合、事前审查与持续监管相结合、企业承诺与社会监督相结合，从产品和服务安全性、可能带来的国家安全风险等方面进行审查。	**第三条** 网络安全审查坚持防范网络安全风险与促进先进技术应用相结合、过程公正透明与知识产权保护相结合、事前审查与持续监管相结合、企业承诺与社会监督相结合，从产品和服务以及数据处理活动安全性、可能带来的国家安全风险等方面进行审查。
第四条 在中央网络安全和信息化委员会领导下，国家互联网信息办公室会同中华人民共和国国家发展和改革委员会、中华人民共和国工业和信息化部、中华人民共和国公安部、中华人民共和国国家安全部、中华人民共和国财政部、中华人民共和国商务部、中国人民银行、国家市场监督管理总局、国家广播电视总局、中国证券监督管理委员会、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，负责制定网络安全审查相关制度规范，组织网络安全审查。	**第四条** 在中央网络安全和信息化委员会领导下，国家互联网信息办公室会同中华人民共和国国家发展和改革委员会、中华人民共和国工业和信息化部、中华人民共和国公安部、中华人民共和国国家安全部、中华人民共和国财政部、中华人民共和国商务部、中国人民银行、国家市场监督管理总局、国家广播电视总局、中国证券监督管理委员会、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，负责制定网络安全审查相关制度规范，组织网络安全审查。
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。	**第五条** 关键信息基础设施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。 关键信息基础设施安全保护工作部门可以制定本行业、本领域预判指南。

网络安全审查办法 （修订草案征求意见稿）	网络安全审查办法 ~~（修订草案征求意见稿）~~
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。 **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、协议等要求产品和服务提供者配合网络安全审查，包括承诺不利用提供产品和服务的便利条件非法获取用户数据、非法控制和操纵用户设备，无正当理由不中断产品供应或必要的技术支持服务等。	**第六条** ~~第七条~~ 对于申报网络安全审查的采购活动，关键信息基础设施运营者应当通过采购文件、协议等要求产品和服务提供者配合网络安全审查，包括承诺不利用提供产品和服务的便利条件非法获取用户数据、非法控制和操纵用户设备，无正当理由不中断产品供应或者必要的技术支持服务等。 **第七条** ~~第六条~~ 掌握超过100万用户个人信息的网络平台运营者赴国外上市，必须向网络安全审查办公室申报网络安全审查。
第八条 运营者申报网络安全审查，应当提交以下材料： （一）申报书； （二）关于影响或可能影响国家安全的分析报告； （三）采购文件、协议、拟签订的合同或拟提交的IPO材料等； （四）网络安全审查工作需要的其他材料。	**第八条** ~~运营者~~当事人申报网络安全审查，应当提交以下材料： （一）申报书； （二）关于影响或者可能影响国家安全的分析报告； （三）采购文件、协议、拟签订的合同或者拟提交的首次公开募股（IPO ~~材料~~）等上市申请文件； （四）网络安全审查工作需要的其他材料。
第九条 网络安全审查办公室应当自收到审查申报材料起，10个工作日内确定是否需要审查并书面通知运营者。	**第九条** 网络安全审查办公室应当自收到符合本办法第八条规定的审查申报材料起~~，~~10个工作日内，确定是否需要审查并书面通知~~运营者~~当事人。
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： （一）产品和服务使用后带来的关键信息基础设施被非法控制、遭受干扰或破坏的风险； （二）产品和服务供应中断对关键信息基础设施业务连续性的危害； （三）产品和服务的安全性、开放性、透明性、来源的多样性，供应渠道的可靠性以及因为政治、外交、贸易等因素导致供应中断的风险； （四）产品和服务提供者遵守中国法律、行政法规、部门规章情况； （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； （七）其他可能危害关键信息基础设施安全和国家数据安全的因素。	**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~~相关对象或者情形的以下国家安全风险~~，主要考虑以下~~因素： （一）产品和服务使用后带来的关键信息基础设施被非法控制、遭受干扰或者破坏的风险； （二）产品和服务供应中断对关键信息基础设施业务连续性的危害； （三）产品和服务的安全性、开放性、透明性、来源的多样性，供应渠道的可靠性以及因为政治、外交、贸易等因素导致供应中断的风险； （四）产品和服务提供者遵守中国法律、行政法规、部门规章情况； （五）核心数据、重要数据或者大量个人信息被窃取、泄露、毁损以及非法利用~~或~~、非法出境的风险； （六）~~国外~~上市~~后~~存在关键信息基础设施~~，~~、核心数据、重要数据或者大量个人信息被~~国~~外国政府影响、控制、恶意利用的风险，以及网络信息安全风险； （七）其他可能危害关键信息基础设施安全、网络安全和~~国家~~数据安全的因素。

网络安全审查办法 （修订草案征求意见稿）	网络安全审查办法 ~~（修订草案征求意见稿）~~
第十一条 网络安全审查办公室认为需要开展网络安全审查的，应当自向运营者发出书面通知之日起 30 个工作日内完成初步审查，包括形成审查结论建议和将审查结论建议发送网络安全审查工作机制成员单位、相关关键信息基础设施保护工作部门征求意见；情况复杂的，可以延长 15 个工作日。	**第十一条** 网络安全审查办公室认为需要开展网络安全审查的，应当自向~~运营者~~当事人发出书面通知之日起 30 个工作日内完成初步审查，包括形成审查结论建议和将审查结论建议发送网络安全审查工作机制成员单位、相关~~关键信息基础设施保护工作~~部门征求意见；情况复杂的，可以延长 15 个工作日。
第十二条 网络安全审查工作机制成员单位和相关关键信息基础设施保护工作部门应当自收到审查结论建议之日起 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、相关关键信息基础设施保护工作部门意见一致的，网络安全审查办公室以书面形式将审查结论通知运营者；意见不一致的，按照特别审查程序处理，并通知运营者。	**第十二条** 网络安全审查工作机制成员单位和相关~~关键信息基础设施保护工作~~部门应当自收到审查结论建议之日起 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、相关~~关键信息基础设施保护工作~~部门意见一致的，网络安全审查办公室以书面形式将审查结论通知~~运营者~~当事人；意见不一致的，按照特别审查程序处理，并通知~~运营者~~当事人。
第十三条 按照特别审查程序处理的，网络安全审查办公室应当听取相关部门和单位意见，进行深入分析评估，再次形成审查结论建议，并征求网络安全审查工作机制成员单位和相关部门意见，按程序报中央网络安全和信息化委员会批准后，形成审查结论并书面通知运营者。	**第十三条** 按照特别审查程序处理的，网络安全审查办公室应当听取相关~~部门和~~单位和部门意见，进行深入分析评估，再次形成审查结论建议，并征求网络安全审查工作机制成员单位和相关部门意见，按程序报中央网络安全和信息化委员会批准后，形成审查结论并书面通知~~运营者~~当事人。
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。	**第十四条** 特别审查程序一般应当在~~3~~90 个~~月~~工作日内完成，情况复杂的可以延长。
第十五条 网络安全审查办公室要求提供补充材料的，运营者、产品和服务提供者应当予以配合。提交补充材料的时间不计入审查时间。	**第十五条** 网络安全审查办公室要求提供补充材料的，~~运营者~~当事人、产品和服务提供者应当予以配合。提交补充材料的时间不计入审查时间。
第十六条 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、数据处理活动以及国外上市行为，由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后，依照本办法的规定进行审查。	**第十六条** 网络安全审查工作机制成员单位认为影响或者可能影响国家安全的网络产品和服务~~、~~以及数据处理活动~~以及国外上市行为~~，由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后，依照本办法的规定进行审查。 为了防范风险，当事人应当在审查期间按照网络安全审查要求采取预防和消减风险的措施。
第十七条 参与网络安全审查的相关机构和人员应严格保护企业商业秘密和知识产权，对运营者、产品和服务提供者提交的未公开材料，以及审查工作中获悉的其他未公开信息承担保密义务；未经信息提供方同意，不得向无关方披露或用于审查以外的目的。	**第十七条** 参与网络安全审查的相关机构和人员应当严格保护~~企业商业秘密和~~知识产权，对~~运营者~~在审查工作中知悉的商业秘密、个人信息，当事人、产品和服务提供者提交的未公开材料，以及~~审查工作中获悉的~~其他未公开信息承担保密义务；未经信息提供方同意，不得向无关方披露或者用于审查以外的目的。
第十八条 运营者或网络产品和服务提供者认为审查人员有失客观公正，或未能对审查工作中获悉的信息承担保密义务的，可以向网络安全审查办公室或者有关部门举报。	**第十八条** ~~运营者~~当事人或者网络产品和服务提供者认为审查人员有失客观公正，或者未能对审查工作中~~获~~知悉的信息承担保密义务的，可以向网络安全审查办公室或者有关部门举报。

网络安全审查办法 （修订草案征求意见稿）	网络安全审查办法 ~~（修订草案征求意见稿）~~
第十九条 运营者应当督促产品和服务提供者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接受举报等形式加强事前事中事后监督。	**第十九条** ~~运营者~~当事人应当督促产品和服务提供者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接受举报等形式加强事前事中事后监督。
第二十条 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》《中华人民共和国数据安全法》的规定处理。	**第二十条** ~~运营者~~当事人违反本办法规定的，依照《中华人民共和国网络安全法》、《中华人民共和国数据安全法》的规定处理。
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。	**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、网络安全和数据安全有重要影响的网络产品和服务。
第二十二条 涉及国家秘密信息的，依照国家有关保密规定执行。	**第二十二条** 涉及国家秘密信息的，依照国家有关保密规定执行。 国家对数据安全审查、外商投资安全审查另有规定的，应当同时符合其规定。
第二十三条 本办法自 2021 年月日起实施，《网络产品和服务安全审查办法（试行）》同时废止。	**第二十三条** 本办法自 ~~2021~~2022 年 2 月 15 日起~~实施，~~施行。2020 年 4 月 13 日公布的《网络~~产品和服务安全审查办法（试行）》~~安全审查办法》（国家互联网信息办公室、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、财政部、商务部、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、国家密码管理局令第 6 号）同时废止。

特别声明

汉坤律师事务所编写《汉坤法律评述》的目的仅为帮助客户及时了解中国或其他相关司法管辖区法律及实务的最新动态和发展，仅供参考，不应被视为任何意义上的法律意见或法律依据。

如您对本期《汉坤法律评述》内容有任何问题或建议，请与汉坤律师事务所以下人员联系：

段志超

电话： +86 10 8516 4123
Email： kevin.duan@hankunlaw.com

蔡克蒙

电话： +86 10 8516 4289
Email： kemeng.cai@hankunlaw.com