上海市通信管理局文件

沪通信管互〔2020〕34号

上海市通信管理局关于开展2020年电信和互联网行业网络安全检查工作的通知

本市各电信企业、互联网企业、域名注册管理和服务机构，各相关单位：

为深入贯彻习近平总书记关于网络安全的系列重要讲话精神，切实做好第三届中国国际进口博览会等重大活动网络安全保障，全面提升本市电信和互联网行业的网络安全防护水平，根据《网络安全法》《通信网络安全防护管理办法》《电信和互联网用户个人信息保护规定》等法律法规和《工业和信息化部办公厅关于做好2020年电信和互联网行业网络数据安全管理工作的通知》《关于开展2020年全市网络安全专项检查的通知》等文件要求，

结合我局职责，决定组织开展2020年上海市电信和互联网行业网络安全检查工作。现将有关要求通知如下:

一、工作目标

紧紧围绕加快推进网络强国建设战略目标，加快落实《网络安全法》有关规定，坚持以查促建、以查促管、以查促防、以查促改，以防攻击、防入侵、防篡改、防窃密、防泄露为重点，深入查找网络安全风险隐患并强化整改，落实电信企业、互联网企业、域名注册管理和服务机构的主体责任，加强网络安全防护能力建设，着力防范重大网络安全风险，保证电信网和公共互联网持续稳定运行和数据安全，确保行业关键信息基础设施安全运行，做好疫情防控、复工复产和第三届中国国际进口博览会网络安全服务保障工作。

二、检查对象

检查对象为在本市行政区域内面向社会提供互联网信息服务的电信企业、互联网企业、域名注册管理和服务机构。重点是上海市各基础电信企业、增值电信企业、工业互联网平台企业、行业关键信息基础设施运营单位、移动互联网App运营单位等。

三、检查内容

（一）通信网络单元定级备案、符合性评测和安全风险评估工作落实情况。以增值电信企业为重点，检查企业的通信网络单元安全防护工作开展情况。各电信和互联网企业要按照《通信网络安全防护管理办法》的规定，对本单位各类信息系统进行网络单元划分和定级备案，并开展符合性评测和安全风险评估。其中，

持有增值电信业务经营许可证的企业应于7月31日前在工业和信息化部“通信网络安全防护管理系统”（https://www.mii-aqfh.cn）报送本单位网络单元的定级信息。市通信管理局将组织专家对各网络单元的定级情况进行评审，并将评审结果通报相应报送单位。各单位应于9月30日前在“网络安全监测预警和信息通报管理系统”（通过上海市通信管理局官方网站（http://shca.miit.gov.cn）首页左侧“行政管理工作系统链接”-“网络安全信息通报”进入）对相应单元的定级评审、符合性评测和安全风险评估结果进行备案。

（二）行业关键信息基础设施清查认定情况。电信和互联网行业各关键信息基础设施运营单位要对本单位运营的关键信息基础设施进行再清查、再认定，按要求通过填报工具填报本单位关键信息基础设施信息，并于7月31日前将填报结果报送市通信管理局审定。各单位应对涉及到国家安全、经济安全、社会稳定、公众健康和安全的重要网络和信息系统予以重点防护，对认定为关键信息基础设施的网络单元，其通信网络安全定级应不低于三级，其安全管理应参照《网络安全法》第三章第二节有关条款实施。市通信管理局将会同有关监管部门，在定级备案和评估检查中，对关键信息基础设施运营单位予以重点监管。

（三）工业互联网平台和联网工控设备安全防护情况。各工业互联网企业应对本单位建设、运营的工业互联网平台进行摸底排查，于7月31日前在市通信管理局“网络安全监测预警和信息通报管理系统”报送相关平台信息。各企业应加强对联网设备、

系统、平台和终端的网络安全防护，重点对工业互联网服务平台、车联网信息服务平台以及联网工控资产、智能网联汽车终端等进行安全检测和自查整改，及时修复安全漏洞。市通信管理局将会同有关主管部门对相关系统、平台的安全状况进行评估和检查。

（四）数据安全和个人信息保护工作情况。按照《电信和互联网用户个人信息保护规定》《工业和信息化部办公厅关于做好2020年电信和互联网行业网络数据安全管理工作的通知》要求，深化行业网络数据安全专项治理行动，重点对App应用违法违规收集使用个人信息情况开展检查。市通信管理局将组织专业技术机构对各企业的App收集使用个人信息合规情况进行评估，并加强对违法违规收集使用个人信息行为的处罚；对强制、过度收集个人信息，未经用户同意、违反法律法规规定和双方约定收集、使用个人信息，发生或可能发生信息泄露、丢失而未采取补救措施，非法出售、非法向他人提供个人信息等行为，依据《网络安全法》从严处罚。

（五）网络安全管理和技术防护情况。检查各互联网企业按照《网络安全法》有关要求建立安全管理体系制度、开展网络安全相关工作的情况。通过远程检测、现场抽测等方式检查企业网络安全技术防护措施的落实情况和有效性，相关软硬件和业务系统是否存在技术漏洞、业务逻辑漏洞，是否已经被植入恶意代码、被非法远程控制或发生数据泄露事件等。重点对近期用户量急剧攀升、业务规模大幅增加的在线新经济型“互联网+”企业加强安全管理，督促相关平台提升安全防护水平。

（六）行业从业人员网络安全意识提升情况。行业内各单位、各企业要按照《关于开展网络安全在线培训的通知》（工网安函〔2020〕533号）有关要求，面向本单位员工加强网络安全教育，开展全员性的安全意识培训。各电信和互联网企业要积极组织本单位从业人员登录工业和信息化部“网络安全在线培训平台”（通过微信搜索并运行“工信人才”微信小程序，从主界面选择“网安学堂”进入培训平台），学习网络安全相关法律法规和基础知识。市通信管理局将对相关工作落实情况进行督查，并从“网安学堂”中选取部分培训课程，通过组织线上考试、开展现场抽测等形式对企业内各类型、各岗位的从业人员进行网络安全知识测试（线上考试具体要求通过市通信管理局“网络安全监测预警和信息通报管理系统”另行通知）。

四、工作安排

（一）动员部署（2020年6月30日前）。对本次网络安全检查工作进行动员部署，统一思想，提高认识，规定时限，明确要求。广泛宣传法律法规、政策制度等相关知识，深入解读电信和互联网行业网络安全检查工作的重点环节，动员相关单位积极参与。

（二）全面自查（2020年7月31日前）。各单位要对照《网络安全法》《通信网络安全防护管理办法》《电信和互联网用户个人信息保护规定》等有关法律法规要求和本次检查重点，对本单位网络信息安全工作进行自查自纠，对自查发现的薄弱环节、安全漏洞和安全风险，要逐一做好记录，对能立即整改的，要边查

边改，对无法立即整改的，要采取防范措施，制定整改计划，确保整改落实。

（三）重点抽查（2020年8月31日前）。市通信管理局将选取部分企业和相关系统，委托专业技术机构通过现场询问、查阅资料、现场检测、远程渗透、源代码检测等方式进行网络安全抽查。对检查发现的薄弱环节、安全漏洞和安全风险，专业技术机构要及时告知相关单位，并指导其进行防范整改；检查完成后要形成检查结果记录报告，上报市通信管理局。对基础电信企业网络和系统的检查结果，将作为2020年省级基础电信企业网络与信息安全责任考核依据。

（四）整改总结（2020年9月30日前）。各企业要对检查发现的薄弱环节和安全风险进行深入整改，并按时向市通信管理局报告整改情况。市通信管理局将组织总结网络安全检查工作情况，对网络安全工作到位的企业予以表扬，对检查发现的问题隐患进行通报；发现存在违反法律法规行为、问题拒不改正或导致危害网络安全等后果的，依法依规给予行政处罚。

五、工作要求

（一）提高认识，加强管理。各单位要深入学习领会习近平总书记关于网络安全的系列重要讲话精神，从国家安全的战略高度出发，充分认识本单位各类网络信息系统的重要性，充分认识新形势下网络攻击威胁的严峻性复杂性，坚持预防为主，强化安全管理，配合主管部门不断完善行业网络安全保障体系。

（二）高度重视，落实责任。各单位要高度重视行业网络安

全检查工作，要按照“谁运行谁负责”的原则，牢固树立本单位网络和系统安全的主责意识，加强组织领导，制定工作方案，明确责任分工，全面深入开展自查自纠工作，积极配合行业主管部门做好监督检查，坚决确保重大活动期间网络安全。

（三）规范检查，严明纪律。检查工作过程中要规范检查方法和程序，避免检查工作影响网络和系统的正常运行；任何检查人员和专业技术机构人员不得向被检查单位收取费用，不得要求被检查单位购买、使用指定的产品和服务；专业技术机构及人员参加安全检查的，要进行严格审查，签订保密承诺书。

（四）强化协同，协调配合。坚持加强协同沟通原则，提倡开展联合检查，避免交叉重复。涉及跨部门、跨行业的网络安全检查，市通信管理局将会同有关主管部门协同开展。各基础电信企业向其他部门提供网络安全相关资料和数据的，应征得市通信管理局同意，并报市通信管理局备案。

特此通知。

上海市通信管理局

2020年6月18日

（联系电话：021-63902000*864）

上海市通信管理局办公室　　2020年6月18日印发