广东省通信管理局

粤通业函〔2019〕190号

关于开展2019年广东省电信和互联网行业网络安全行政检查工作的通知

省内各基础电信企业、各互联网企业、各域名从业机构：

为深入贯彻落实习近平总书记关于网络安全的系列重要讲话精神，切实做好庆祝新中国成立70周年网络安全保障工作，全面提升电信和互联网行业网络安全防护水平，结合工业和信息化部《关于做好2019年电信和互联网行业网络安全行政检查工作的通知》（工网安函〔2019〕615号）要求，我局现组织开展2019年广东电信和互联网行业网络安全行政检查工作。现将有关事项通知如下：

一、总体要求

紧紧围绕加快推进网络强国建设战略目标，加快落实《中华人民共和国网络安全法》，以防攻击、防入侵、防篡改、防窃密为重点，深入查找网络安全风险隐患并强化整改，落实基础电信企业、域名从业机构、互联网服务提供者的主体责任，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

证我省电信网和公共互联网持续稳定运行和数据安全。

二、检查对象

检查对象为省内基础电信企业、互联网企业、域名从业机构运营的电信和互联网行业网络基础设施，收集、存储与处理用户信息和网络数据的重要信息系统，其中互联网企业重点检查移动应用分发平台（App 应用商店）、互联网数据中心、内容分发平台、工业互联网平台、网约车平台、直播平台、游戏互动平台、电商平台企业等互联网企业，域名从业机构检查域名注册、域名解析等系统。

三、检查内容

（一）检查各单位落实《中华人民共和国网络安全法》《通信网络安全防护管理办法》等法律法规情况，电信和互联网安全防护体系系列标准符合情况，主要包括：

1.网络安全管理落实情况。重点检查内部安全管理制度制定与落实、网络安全事件预案、网络安全责任部门和人员履职尽责情况，本单位网络与系统的定级备案、符合性评测和安全风险评估工作开展情况，网络安全教育和培训开展情况等。

2.网络安全防护技术手段。重点检查网络隔离、身份鉴别、访问控制、口令管理、边界防护、数据保护、容灾备份、安全审计、日志留存等网络安全防护技术措施的标准符合性和有效性，以及网络安全监测手段的建设和运行情况。

3.仍然存在的漏洞等风险隐患。重点检查软硬件系统存在的漏洞（特别是 Struts2 漏洞）、弱口令、后门、被植入恶意程

序、网站被篡改、被非法入侵、被非法远程控制等。

（二）检查各单位信息安全管理的落实情况，根据《电信业务经营许可管理办法》《互联网新技术新业务信息安全评估管理办法（试行）》(工信部保〔2012〕117 号)《互联网信息服务管理办法》《非经营性互联网信息服务备案管理办法》，重点检查企业违法信息监测处置机制、新技术新业务的安全评估以及相关备案信息准确性和应急电话有效性情况。

（三）检查各单位数据安全以及用户个人信息保护的落实情况。根据《中华人民共和国网络安全法》《电信和互联网用户个人信息保护规定》《电信和互联网服务用户个人信息保护分级指南》和《2019 年基础电信企业数据安全合规性评估要点》（工网安函〔2019〕653 号），重点检查数据安全管理制度的落实情况、数据的分级管理、重要数据的安全防护、规范开展第三方合作、用户账号注销服务、隐私政策和个人信息收集情况等。

四、工作安排

（一）自查自纠（7 月 15 日前完成）。各单位要认真落实自查工作：一是要全面梳理所有正式上线运行的网络与系统，7 月 10 日前，在“通信网络安全防护管理系统”（https://www.mii-aqfh.cn）完成定级备案，并核实已有备案信息的内容，对不准确、不完整的备案信息予以补正，定级备案完成情况将作为我局检查评估的重点内容。二是要组织开展本单位网络与系统的自查评估，及时整改并做好自查总结。7 月

15日前，基础电信企业、域名从业机构和互联网公司向我局书面上报自查总结报告。

（二）检查评估（即日起至8月中旬）。我局将委托专业技术机构分别进行远程检测及现场检查：

1.对全省获得电信业务经营许可企业的网站及重要政府网站采取抽测方式进行远程检测；

2.重点选择基础电信企业、电商平台、工业互联网平台、互联网数据中心、网约车平台以及移动应用分发平台等企业采取现场访谈、资料查阅、检查检测等方式进行现场检查。

（三）整改问责。对检查过程中发现的问题，各单位要高度重视，认真整改，及时向我局报告整改情况。对基础电信企业省级公司和专业公司，将其网络和系统检查结果作为2019年省级基础电信企业和专业公司网络与信息安全责任考核依据。对域名从业机构、互联网企业，发现存在违反法律法规行为的，我局将依法给予行政处罚并纳入不良名单和失信名单。

各单位要强化问题导向，根据检查重点加强自查评估，增强问题发现和整改能力，举一反三，切实提升网络安全防护能力，健全网络安全问题闭环管理机制。

广东省通信管理局

2019年6月20日