工业和信息化部
关于加强电信和互联网行业网络安全工作的指导意见

工信部保〔2014〕368号

各省、自治区、直辖市通信管理局，中国电信集团公司、中国移动通信集团公司、中国联合网络通信集团有限公司，国家计算机网络应急技术处理协调中心，工业和信息化部电信研究院、通信行业职业技能鉴定指导中心，中国通信企业协会、中国互联网协会，各互联网域名注册管理机构，有关单位：

近年来，各单位认真贯彻落实党中央、国务院决策部署及工业和信息化部的工作要求，在加强网络基础设施建设、促进网络经济快速发展的同时，不断强化网络安全工作，网络安全保障能力明显提高。但也要看到，当前网络安全形势十分严峻复杂，境内外网络攻击活动日趋频繁，网络攻击的手法更加复杂隐蔽，新技术新业务带来的网络安全问题逐渐凸显。新形势下电信和互联网行业网络安全工作存在的问题突出表现在：重发展、轻安全思想普遍存在，网络安全工作体制机制不健全，网络安全技术能力和手段不足，关键软硬件安全可控程度低等。为有效应对日益严峻复杂的网络安全威胁和挑战，切实加强和改进网络安全工作，进一步提高电信和互联网行业网络安全保障能力和水平，提出以下意见。

一、总体要求

认真贯彻落实党的十八大、十八届三中全会以及中央网络安全和信息化领导小组第一次会议关于维护网络安全的有关精神，坚持以安全保发展、以发展促安全，坚持安全与发展工作统一谋划、统一部署、统一推进、统一实施，坚持法律法规、行政监管、行业自律、技术保障、公众监督、社会教育相结合，坚持立足行业、服务全局，以提升网络安全保障能力为主线，以完善网络安全保障体系为目标，着力提高网络基础设施和业务系统安全防护水平，增强网络安全技术能力，强化网络数据和用户信息保护，推进安全可控关键软硬件应用，为维护国家安全、促进经济发展、保护人民群众利益和建设网络强国发挥积极作用。

二、工作重点

（一）**深化网络基础设施和业务系统安全防护**。认真落实《通信网络安全防护管理办法》（工业和信息化部令第11号）和通信网络安全防护系列标准，做好定级备案，严格落实防护措施，定期开展符合性评测和风险评估，及时消除安全隐患。加强网络和信息资产管理，全面梳理关键设备列表，明确每个网络、系统和关键设备的网络安全责任部门和责任人。合理划分网络和系统的安

全域，理清网络边界，加强边界防护。加强网站安全防护和企业办公、维护终端的安全管理。完善域名系统安全防护措施，优化系统架构，增强带宽保障。加强公共递归域名解析系统的域名数据应急备份。加强网络和系统上线前的风险评估。加强软硬件版本管理和补丁管理，强化漏洞信息的跟踪、验证和风险研判及通报，及时采取有效补救措施。

（二）**提升突发网络安全事件应急响应能力**。认真落实工业和信息化部《公共互联网网络安全应急预案》，制定和完善本单位网络安全应急预案。健全大规模拒绝服务攻击、重要域名系统故障、大规模用户信息泄露等突发网络安全事件的应急协同配合机制。加强应急预案演练，定期评估和修订应急预案，确保应急预案的科学性、实用性、可操作性。提高突发网络安全事件监测预警能力，加强预警信息发布和预警处置，对可能造成全局性影响的要及时报通信主管部门。严格落实突发网络安全事件报告制度。建设网络安全应急指挥调度系统，提高应急响应效率。根据有关部门的需求，做好重大活动和特殊时期对其他行业重要信息系统、政府网站和重点新闻网站等的网络安全支援保障。

（三）**维护公共互联网网络安全环境**。认真落实工业和信息化部《木马和僵尸网络监测与处置机制》、《移动互联网恶意程序监测与处置机制》，建立健全钓鱼网站监测与处置机制。在与用户签订的业务服务合同中明确用户维护网络安全环境的责任和义务。加强木马病毒样本库、移动恶意程序样本库、漏洞库、恶意网址库等建设，促进行业内网络安全威胁信息共享。加强对黑客地下产业利益链条的深入分析和源头治理，积极配合相关执法部门打击网络违法犯罪。基础电信企业在业务推广和用户办理业务时，要加强对用户网络安全知识和技能的宣传辅导，积极拓展面向用户的网络安全增值服务。

（四）**推进安全可控关键软硬件应用**。推动建立国家网络安全审查制度，落实电信和互联网行业网络安全审查工作要求。根据《通信工程建设项目招标投标管理办法》（工业和信息化部令第 27 号）的有关要求，在关键软硬件采购招标时统筹考虑网络安全需要，在招标文件中明确对关键软硬件的网络安全要求。加强关键软硬件采购前的网络安全检测评估，通过合同明确供应商的网络安全责任和义务，要求供应商签署网络安全承诺书。加大重要业务应用系统的自主研发力度，开展业务应用程序源代码安全检测。

（五）**强化网络数据和用户个人信息保护**。认真落实《电信和互联网用户个人信息保护规定》（工业和信息化部令第 24 号），严格规范用户个人信息的收集、存储、使用和销毁等行为，落实各个环节的安全责任，完善相关管理制

度和技术手段。落实数据安全和用户个人信息安全防护标准要求，完善网络数据和用户信息的防窃密、防篡改和数据备份等安全防护措施。强化对内部人员、合作伙伴的授权管理和审计，加大违规行为惩罚力度。发生大规模用户个人信息泄露事件后要立即向通信主管部门报告，并及时采取有效补救措施。

（六）**加强移动应用商店和应用程序安全管理**。加强移动应用商店、移动应用程序的安全管理，督促应用商店建立健全移动应用程序开发者真实身份信息验证、应用程序安全检测、恶意程序下架、恶意程序黑名单、用户监督举报等制度。建立健全移动应用程序第三方安全检测机制。推动建立移动应用程序开发者第三方数字证书签名和应用商店、智能终端的签名验证和用户提示机制。完善移动恶意程序举报受理和黑名单共享机制。加强社会宣传，引导用户从正规应用商店下载安装移动应用程序、安装终端安全防护软件。

（七）**加强新技术新业务网络安全管理**。加强对云计算、大数据、物联网、移动互联网、下一代互联网等新技术新业务网络安全问题的跟踪研究，对涉及提供公共电信和互联网服务的基础设施和业务系统要纳入通信网络安全防护管理体系，加快推进相关网络安全防护标准研制，完善和落实相应的网络安全防护措施。积极开展新技术新业务网络安全防护技术的试点示范。加强新业务网络安全风险评估和网络安全防护检查。

（八）**强化网络安全技术能力和手段建设**。深入开展网络安全监测预警、漏洞挖掘、恶意代码分析、检测评估和溯源取证技术研究，加强高级可持续攻击应对技术研究。建立和完善入侵检测与防御、防病毒、防拒绝服务攻击、异常流量监测、网页防篡改、域名安全、漏洞扫描、集中账号管理、数据加密、安全审计等网络安全防护技术手段。健全基于网络侧的木马病毒、移动恶意程序等监测与处置手段。积极研究利用云计算、大数据等新技术提高网络安全监测预警能力。促进企业技术手段与通信主管部门技术手段对接，制定接口标准规范，实现监测数据共享。加强与网络安全服务企业的合作，防范服务过程中的风险，在依托安全服务单位开展网络安全集成建设和风险评估等工作时，应当选用通过有关行业组织网络安全服务能力评定的单位。

三、保障措施

（一）**加强网络安全监管**。通信主管部门要切实履行电信和互联网行业网络安全监管职责，不断健全网络安全监管体系，积极推动关键信息基础设施保护、网络数据保护等网络安全相关立法，进一步完善网络安全防护标准和有关工作机制；要加大对基础电信企业的网络安全监督检查和考核力度，加强对互联网域名注册管理和服务机构以及增值电信企业的网络安全监管，推动建立电

信和互联网行业网络安全认证体系。国家计算机网络应急技术处理协调中心和工业和信息化部电信研究院等要加大网络安全技术、资金和人员投入，大力提升对通信主管部门网络安全监管的支撑能力。

（二）**充分发挥行业组织和专业机构的作用**。充分发挥行业组织支撑政府、服务行业的桥梁纽带作用，大力开展电信和互联网行业网络安全自律工作。支持相关行业组织和专业机构开展面向行业的网络安全法规、政策、标准宣贯和知识技能培训、竞赛，促进网络安全管理和技术交流；开展网络安全服务能力评定，促进和规范网络安全服务市场健康发展；建立健全网络安全社会监督举报机制，发动全社会力量参与维护公共互联网网络安全环境；开展面向社会公众的网络安全宣传教育活动，提高用户的网络安全风险意识和自我保护能力。

（三）**落实企业主体责任**。相关企业要从维护国家安全、促进经济社会发展、保障用户利益的高度，充分认识做好网络安全工作的重要性、紧迫性，切实加强组织领导，落实安全责任，健全网络安全管理体系。基础电信企业主要领导要对网络安全工作负总责，明确一名主管领导具体负责、统一协调企业内部网络安全各项工作；要加强集团公司、省级公司网络安全管理专职部门建设，加强专职人员配备，强化专职部门的网络安全管理职能，切实加大企业内部网络安全工作的统筹协调、监督检查、责任考核和责任追究力度。互联网域名注册管理和服务机构、增值电信企业要结合实际健全内部网络安全管理体系，配备网络安全管理专职部门和人员，保证网络安全责任落实到位。

（四）**加大资金保障力度**。基础电信企业要制定本企业网络安全专项规划，在加大网络和业务发展投入的同时，同步加大网络安全保障资金投入，并将网络安全经费纳入企业年度预算。互联网域名注册管理和服务机构、增值电信企业要结合实际加大网络安全资金投入力度。

（五）**加强人才队伍建设**。基础电信企业要积极开展网络安全专业岗位职业技能鉴定工作，建立健全网络安全专业岗位持证上岗制度；加强网络安全培训，把相关培训纳入员工培训计划；积极组织和参与网络安全知识技能竞赛，形成培养、选拔、吸引和使用网络安全人才的良性机制。