中国通信企业协会文件

通企〔2020〕22号

关于开展网络安全防护能力评定试点工作的通知

中国电信集团有限公司、中国移动通信集团有限公司、中国联合网络通信集团有限公司、中国铁塔股份有限公司、中国广播电视网络有限公司，各相关单位：

为深入贯彻《网络安全法》，认真落实工业和信息化部《通信网络安全防护管理办法》（工业和信息化部令第11号）、《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）、《信息通信网络与信息安全规划（2016-2020）》等相关要求，加快网络安全防护能力评定体系建设，推动网络安全防护水平不断提高，中国通信企业协会决定组织开展网络安全防护能力评定试点工作（以下简称：评定工作），由中国通信企业协会通信网络安全专业委员会（以下简称：网络安全专委会）

负责具体实施。评定工作自2020年3月27日起试行，为期一年。现将有关事项通知如下：

一、评定依据

按照《网络安全法》和工业和信息化部《通信网络安全防护管理办法》（工业和信息化部令第11号）、《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）等相关要求，依托电信和互联网行业网络安全防护工作体系，依据网络安全防护系列标准，结合网络和系统安全定级备案，参照对网络和系统安全管理和技术措施进行评测的思路和方法开展评定工作。

二、评定对象

电信网和互联网的网络和系统、广电网络中与经营电信业务相关的网络和系统。

三、组织机构

评定工作遵循“先试点，后推广”的思路，试点期间由网络安全专委会和中国信息通信研究院（以下简称“信通院”）负责方案制定和实施。

评定工作机构设在中国通信企业协会，具体机构包括：评定工作秘书处、专家委员会、标准编制组、第三方评定机构。评定工作秘书处常设在网络安全专委会，具体负责日常各项组织和管理工作。

第三方评定机构负责对网络和系统安全防护能力开展合规性评测、隐患排查、渗透测试等技术测试，试点期间由信通院和国家计算机网络应急技术处理协调中心（CNCERT）承担。后期推

广阶段，第三方评定工作逐步向其它专业机构开放。

四、评定流程

试点期间评定流程包括评定申请、评定实施、专家评审、结果公布、证后管理五个环节，具体如下：

（一）评定申请

1、网络和系统运营企业向评定工作秘书处提出评定申请，明确需开展第三方评定的网络和系统名称；

2、网络和系统运营企业根据评定工作秘书处回复的申请向协会授权的第三方评定机构提出评定申请。

（二）评定实施

第三方评定机构根据申请对网络和系统开展评定并出具结果。

（三）专家评审

评定工作秘书处根据第三方评定机构对网络和系统运营企业的网络和系统评定结果给出结论，并组织有关专家对评定结果进行评审，提交中国通信企业协会最终审核。

（四）结果公布

由中国通信企业协会对专家评审结果进行最终审核后在官网公示，并为通过能力评定的网络和系统颁发网络安全防护能力评定证书。

（五）证后管理

网络安全防护能力评定证书采取年检制度，评定工作秘书处每年对获证企业进行一次年检，采用书面审查、现场核查相结合的方式。

五、申请材料提交

申请企业向评定工作秘书处邮寄提交盖章后的《网络安全防护能力评定申请表》（纸质版），并将《网络安全防护能力评定申请表》（电子版）发送至指定工作邮箱：ccpc@caict.ac.cn。

六、收费标准

评定工作试点期间只收取成本费用，不以盈利为目的，具体收费标准另行通知。

联系单位：中国通信企业协会

联系地址：北京市西城区月坛南街11号213室

联系人：郝强 18810916366　　许寒 13810891334

附件：1. 网络安全防护能力评定试点工作实施方案

2. 网络安全防护能力评定申请表

中国通信企业协会

2020年3月31日

附件 1

网络安全防护能力评定试点工作实施方案

一、政策依据

（一）《网络安全法》

第十一条 网络相关行业组织按照章程，加强行业自律，制定网络安全行为规范，指导会员加强网络安全保护，提高网络安全保护水平，促进行业健康发展。

第十七条 国家推进网络安全社会化服务体系建设，鼓励有关企业、机构开展网络安全认证、检测和风险评估等安全服务。

（二）《通信网络安全防护管理办法》（工业和信息化部令第11号）

第四条 中华人民共和国工业和信息化部（以下简称工业和信息化部）负责全国通信网络安全防护工作的统一指导、协调和检查，组织建立健全通信网络安全防护体系，制定通信行业相关标准。

第七条 电信管理机构应当组织专家对通信网络单元的分级情况进行评审。

通信网络运行单位应当根据实际情况适时调整通信网络单元的划分和级别，并按照前款规定进行评审。

第十六条 通信网络运行单位可以委托专业机构开展通信网

络安全评测、评估、监测等工作。

第十八条 电信管理机构可以委托专业机构开展通信网络安全检查活动。

（三）《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）

明确提出“推动建立电信和互联网行业网络安全认证体系”。

（四）《信息通信网络与信息安全规划（2016-2020）》

提出“建立信息通信领域网络与信息安全标准认证体系”。

二、目标和定位

目标：加强行业自律，制定网络安全防护行为规范，指导行业和企业加强网络安全保护，提高网络安全防护水平。建立起基于标准的、第三方的网络和系统安全防护能力评定制度和体系，规范并提升网络安全服务等网络和系统安全防护能力建设的相关工作，促进网络和系统运营企业安全防护水平和质量不断提高，推动行业健康发展。

定位：政府引导，行业自律，自愿参与。

三、基本思路

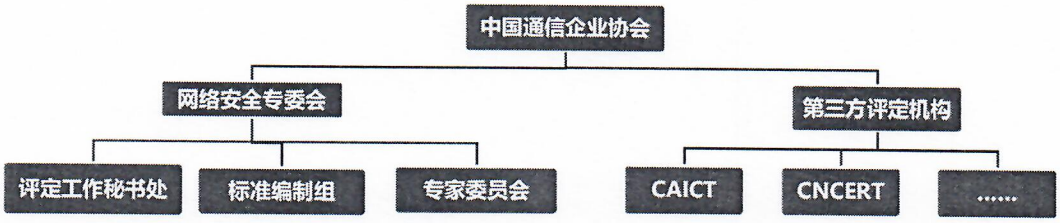
按照《网络安全法》和工业和信息化部《通信网络安全防护管理办法》（工业和信息化部令第11号）、《关于加强电信和互联网行业网络安全工作的指导意见》（工信部保〔2014〕368号）等相关要求，依托行业网络安全防护工作体系，依据网络安全防护系列标准，结合网络和系统安全定级备案，参照对网络和系统

网络安全管理和技术措施进行评测的思路和方法，对电信网、互联网、广电网络的网络和系统进行评定，并对通过评定的网络和系统颁发证书。

评定工作按照“先试点，后推广”的思路，试点期间由中国通信企业协会通信网络安全专业委员会（以下简称“网络安全专委会”）和中国信息通信研究院（以下简称“信通院”）负责方案制定和实施。

四、组织机构

评定工作机构设在中国通信企业协会，具体机构包括：评定工作秘书处、专家委员会、标准编制组、第三方评定机构。评定工作秘书处常设在网络安全专委会，具体负责日常各项组织和管理工作。



评定工作秘书处具体负责日常各项组织和管理工作，包括受理评定申请、对申请材料进行审核、第三方评定机构资质管理、接收评定结果、组织专家评审、证书发放、证后管理和检查，接受网络和系统运营企业对第三方评定机构的投诉并组织调查处理等相关工作。

标准编制组负责制定网络安全防护能力评定有关标准性文件，包括评定管理方案、评测打分方案、证后管理方案等，并在评定试点过程中对相关标准进行完善。标准编制组成员由评定工作秘书处组织。

第三方评定机构负责对网络和系统安全防护能力开展合规性评测、隐患排查、渗透测试等技术测试，试点期间由信通院和国家计算机网络应急技术处理协调中心（CNCERT）承担。后期推广阶段，第三方评定工作逐步向其它专业机构开放。第三方评定机构应具备网络安全服务能力评定风险评估类二级及以上资质。

专家委员会负责对第三方评定机构的评定结果进行评审，专家委员会成员由政府部门、社会团体、安全企业、专业机构、科研院校等单位的领导和专家组成。

五、能力评定流程

试点期间评定流程包括评定申请、评定实施、专家评审、结果公布、证后管理五个环节，具体如下：

（一）评定申请

1、网络和系统运营企业向评定工作秘书处提出评定申请，明确需开展第三方评定的网络和系统名称；

2、网络和系统运营企业根据评定工作秘书处回复的申请向协会授权的第三方评定机构提出评定申请。

（二）评定实施

第三方评定机构根据申请对网络和系统开展评定并出具结

果。

（三）专家评审

评定工作秘书处根据第三方评定机构对网络和系统运营企业的网络和系统评定结果给出结论，并组织有关专家对评定结果进行评审，提交中国通信企业协会最终审核。

（四）结果公布

由中国通信企业协会对专家评审结果进行最终审核后在官网公示结果，并为通过能力评定的网络和系统颁发网络安全防护能力评定证书。

（五）证后管理

网络安全防护能力评定证书采取年检制度，评定工作秘书处每年对获证企业进行一次年检，采用书面审查、现场核查相结合的方式。其中，网络安全防护能力（二级）评定证书有效期3年，有效期内需要年检，年检采用书面审查方式。网络安全防护能力（三级）评定证书有效期2年，有效期内需要年检，年检采用书面审查、现场核查相结合方式。年检结果分为合格或不合格；不合格的，限期整改，评定机构进行核查；对于整改仍不合格的，取消能力评定证书。年检结果视情上报行业主管部门和基础电信运营企业。

六、试点对象

评定工作试点期间，网络和系统运营企业可申请对网络安全防护定级备案二级及以上的以下对象开展网络安全防护能力第

三方评定的试点工作。

电信网和互联网重点网络和系统、广电网络中与经营电信业务相关的典型网络和系统，包括但不限于：

（一）关键信息基础设施类

1. IP 承载网

2. 域名系统

3. 通信铁塔等基站设施

（二）新技术新业务类

1. 云服务、大数据平台

2. 互联网信息服务系统（网站、增值电信业务系统）

3. 区块链平台

七、申请材料提交

申请企业向评定工作秘书处邮寄提交盖章后的评定申请表（纸质版），并将评定申请表（电子版）发送指定工作邮箱：ccpc@caict.ac.cn。

八、评定标准及打分方案

（一）评定标准

网络安全防护能力评定内容主要包括：网络和系统有关网络安全管理制度情况、组织机构和人员配置情况，网络安全防护技术措施情况、渗透测试发现的漏洞隐患情况等，其中，管理制度等要求依据国家和行业网络安全法律法规规章制定，技术和管理参考标准包括但不限于：

1、YD/T 1756-2008 电信网和互联网管理安全等级保护要求

2、YD/T 1757-2008 电信网和互联网管理安全等级保护检测要求

3、YD/T 1746-2013 IP 承载网安全防护要求

4、YD/T 1747-2013 IP 承载网安全防护检测要求

5、YD/T 2052-2009 域名系统安全防护技术要求

6、YD/T 2053-2009 域名系统安全防护检测要求

7、YD/T 3157-2016 公有云服务安全防护要求

8、YD/T 3158-2016 公有云服务安全防护检测要求

9、YD/T 2243-2011 电信网和互联网信息服务业务系统安全防护要求

10、YD/T 2244-2011 电信网和互联网信息服务业务系统安全防护检测要求

11、YD/T 2698-2014 电信网和互联网安全防护基线配置要求及检测要求 网络设备

12、YD/T 2699-2014 电信网和互联网安全防护基线配置要求及检测要求 安全设备

13、YD/T 2700-2014 电信网和互联网安全防护基线配置要求及检测要求 数据库

14、YD/T 2701-2014 电信网和互联网安全防护基线配置要求及检测要求 操作系统

15、YD/T 2702-2014 电信网和互联网安全防护基线配置要求及检测要求 中间件

16、YD/T 2703-2014 电信网和互联网安全防护基线配置要求及检测要求 web 应用系统

（二）评分方案

为直观反映网络和系统的安全防护能力，基于电信网和互联网安全防护技术要求系列标准以及网络安全管理能力要求有关标准，制定本评分方法。

1、评定评分计算公式

评定综合评分＝技术评定得分×60%＋网络安全管理能力要求评定得分×40%;

其中，技术评定评分和网络安全管理能力要求评定评分均采用百分制。

2、评分方法

评定评分依据网络和系统技术评定表、网络安全管理能力评定表中所列制度、措施的符合情况计分，其中每个评定项对应分值，由 100 分除以技术评定表中评定项总数所得。

例如，技术评定表中共有 80 个评定项，则每个评定项的分值为 1.25（100÷80）。

（三）评定结果评分方法

评定根据技术评定得分、网络安全管理能力要求评定得分情

况给出评定结果。其中，对于技术评定、网络安全管理能力要求评定两项分项得分85分以上，综合评分90分以上的网络和系统，予以通过。

附件 2

编号：

中国通信企业协会

网络安全防护能力评定申请表

申请单位（公章）：_____

填写日期：_____

申请单位名称（中文）					
注册地址			办公地址		
法人代表		单位职务		联系方式	
单位性质		成立时间		职工人数	
联系人			单位职务		
手机号码			固定电话		
E-MAIL			传真号码		
申请单位意见： 单位盖章： 日　期：					
评定工作秘书处意见： 单位盖章： 日　期：					

附：1. 企业营业执照

2. 申请开展能力评定的网络和系统列表

抄送：中国信息通信研究院，国家计算机网络应急技术处理协调中心

中国通信企业协会秘书处　　2020 年 3 月 31 日印发