工业和信息化部司局简函

工网安函〔2025〕331号

工业和信息化部网络安全管理局关于规范开展2025年信息通信网络安全防护工作的函

各省、自治区、直辖市通信管理局，电信业务经营者、互联网域名服务提供者：

为深入贯彻落实《网络安全法》《关键信息基础设施安全保护条例》《通信网络安全防护管理办法》等法律法规和政策文件要求（见附件1），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，进一步提升信息通信网络安全防护水平，保障信息通信网络安全稳定运行。现将有关要求通知如下。

一、落实网络安全防护措施的三同步要求

电信业务经营者、互联网域名服务提供者（以下统称信息通信网络运行单位）要按照网络安全防护同规划同建设同运行实施要求，对新建、改建、扩建、已建的信息通信网络，实施网络安全防护措施的同步规划、同步建设、同步运行。规划阶段要开展安全需求分析，形成安全总体方案和安全建设方案。建设阶段要细化设计方案，落实安全管理和技术要求，项目完成后组织验收并形成验收和检测报告。运行阶段

要做好运行监控、变更管控、事件响应、安全检测，持续提升安全能力，确保安全保障工作的有效性。网络安全防护同规划、同建设、同运行相关材料应做好留存备查。

二、提升信息通信网络单元定级备案率和准确率

信息通信网络运行单位要按照电信网和互联网网络安全防护定级备案实施要求，全面系统梳理本单位已正式投入运行的信息通信网络单元划分、定级备案、资产纳管情况，核查各信息通信网络单元的定级备案信息、资产信息等的真实性、完整性和准确性，于2025年8月底前完成存量信息通信网络单元的全面核查，并通过通信网络安全防护管理系统向电信主管部门更新备案信息（模板见附件2）。其他有关部门要求提供相关定级备案信息的，运行单位需及时向电信主管部门报告，由电信主管部门统一出口。

三、加强信息通信网络安全符合性评测

信息通信网络运行单位要按照电信网和互联网安全防护系列标准要求（安全防护相关标准、符合性评测报告模板及填报注意事项可在通信网络安全防护管理系统的“文件下载中心”查看和下载），采取与信息通信网络单元类别、安全级别相适应的身份鉴别、访问控制、边界防护、安全审计等网络安全防护管理和技术措施，并按照规定频次自行或委托专业机构开展网络安全防护系列标准的符合性评测。其中，三级及以上信息通信网络单元每年开展一次，二级信息通信网络单元每两年开展一次，信息通信网络单元的划分和级别

调整的，在九十日内重新进行符合性评测，评测结束三十日内完成系统填报和证明材料提交。

四、强化信息通信网络安全风险评估

信息通信网络运行单位要按照电信网和互联网安全风险评估规范开展安全风险评估，及时发现并消除重大网络安全隐患和漏洞。风险评估要贯穿信息通信网络单元规划建设、实施运维等全生命周期，在信息通信网络单元上线前充分评估安全措施有效性，上线后按照符合性评测规定的频次要求开展常态化评估，系统化识别、分析风险，采取应对举措。在系统发生重大变更时，或在国家重大活动举办前，按照电信主管部门的要求开展评估。评估结束三十日内，将评估结果、隐患处理情况或者处理计划通过通信网络安全防护管理系统报送电信主管部门（模板见附件 3）。

五、做好暴露面风险管理

信息通信网络运行单位要系统梳理互联网暴露面，包括承载电信业务、企业办公、业务支撑等的各类信息通信网络单元互联网出入口，严控出入口数量，做好边界隔离和安全防护。基础电信企业省级公司办公网互联网出入口数量原则上不超过 2 个，有特殊情况的需向集团公司报备，加强暴露面监测和安全管理。统计办公网互联网出入口，以及接入在用的各类信息通信网络单元的虚拟专用网络（VPN）、零信任网络的情况，形成互联网暴露面信息列表（模板见附件 4），与本年度网络安全防护工作总结报告同步提交。

六、加强网络安全威胁监测

信息通信网络运行单位要按照公共互联网网络安全威胁监测与处置要求，做好常态化网络安全威胁监测与处置。建设网络安全威胁监测与处置技术手段，在互联网出入口、网络边界等网络关键节点部署攻击监测设备，基于流量监测、网元自身安全组件监测、日志采集分析等，提升恶意程序传播、漏洞攻击利用等网络威胁精准监测、分析研判能力，及时发现并处置各类风险隐患与威胁。加强威胁信息共享，在电信主管部门统一指导下，合力形成行业一体的协同联动防护机制，做到安全威胁一处发现、全网处置。

七、强化网络安全事件应急处置

信息通信网络运行单位要按照公共互联网网络安全突发事件应急预案要求，提升网络安全突发事件应急处置能力。制定并更新完善本单位网络安全应急预案，做好重大活动网络安全保障准备。定期参与或自行组织开展针对性、实战化网络安全事件应急演练，不断健全网络安全事件报告和应急处置机制。严格落实突发事件报告制度，发生重大网络安全事件或者发现重大网络安全威胁的，立即向工业和信息化部网络安全管理局报告，发生较大或一般网络安全事件的，立即向属地通信管理局报告，并在事件应急响应结束后十个工作日内，将总结报告报电信主管部门。

八、报送要求

各信息通信网络运行单位要切实发挥主体责任，积极配

合，切实推进网络安全防护工作的落地实施，并于2025年11月底前将本年度网络安全防护工作开展情况（包括定级备案、符合性评测、安全风险评估、暴露面信息、应急预案及演练情况），正式报送至电信主管部门（模板见附件5）。其中，基础电信企业各省（自治区、直辖市）子公司、分公司向属地通信管理局、基础电信企业集团公司报送，基础电信企业集团公司、专业公司及其他信息通信网络运行单位向工业和信息化部网络安全管理局报送。

附件：1.信息通信网络安全防护工作有关依据

2.（网络单元名称）定级报告（模板）

3.（网络单元名称）风险评估报告（模板）

4.互联网暴露面信息（模板）

5.（运行单位）安全防护工作报告（模板）

工业和信息化部网络安全管理局

2025年4月24日

（联系人及电话：王梅芳 68206192）

附件 1

信息通信网络安全防护工作有关政策文件

一、《中华人民共和国网络安全法》

二、《关键信息基础设施安全保护条例》

三、《通信网络安全防护管理办法》（部令第11号）

四、《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）

五、《公共互联网网络安全威胁监测与处置办法》（工信部网安〔2017〕202号）

六《公共互联网网络安全突发事件应急预案》（工信部网安〔2017〕281号）

七、《网络产品安全漏洞管理规定》(工信部联网安〔2021〕66号）

附件 2

（网络单元名称）定级报告（模板）

一、基本情况

此部分应描述网络单元以下相关内容:

（一）概述

描述该网络单元的业务/应用范围、服务范围、用户类型等。

（二）管理情况

描述该网络单元所属单位的基本情况、安全管理架构等内容。

（三）技术情况

描述网络单元的网络拓扑结构、硬件设备的部署情况和基本信息、网络边界划分等。

二、安全等级的确定

此部分应说明如何确定网络单元的安全等级:

（一）详细阐述“社会影响力、规模和服务范围、所提供服务的重要性”三个定级要素赋值的过程和理由，每一个定级要素的赋值范围是从1至5的整数。

（二）根据三个定级要素的赋值计算得出安全等级。

根据网络单元的社会影响力I、规模和服务范围R、所提

供服务重要性V三个定级要素的赋值，采用以下公式来计算网络单元的安全等级值:

$$k = \text{Round1}\{\text{Log}_2[\alpha\times 2^{I}+\beta\times 2^{R}+\gamma\times 2^{V}]\}$$

其中，k代表安全等级值，I代表社会影响力赋值、R代表规模和服务范围赋值、V代表所提供服务的重要性赋值，Round1{}表示四舍五入处理，保留1位小数，Log_2[]表示取以2为底的对数，α、β、γ分别表示网络单元的社会影响力、规模和服务范围、所提供服务的重要性赋值所占的权重，分别为1/3、1/3、1/3。

计算所得网络单元的安全等级值与安全等级的映射关系如下表所示:

安全等级值k	安全等级
$1\leq k<1.5$	第1级
$1.5\leq k<2.5$	第2级
$2.5\leq k<4$	第3级
$4\leq k<4.5$	第4级
$4.5\leq k\leq 5$	第5级

附件 3

（网络单元名称）安全风险评估报告（模板）

一、概述

包含评估目的、依据、评估过程等内容。

二、被评估对象描述

包含评估内容、范围等内容。

三、风险分析及评估方法

包含风险分析模型、风险评估方法等内容。

四、风险识别结果

包含业务识别、资产识别、威胁识别、脆弱性识别和已有安全措施确认等相关内容。

五、风险分析结果

包含风险值计算过程、分析结果等内容。

六、风险评价

包含评价准则、评价结果等内容。

七、风险评估总结

包含评估结果、处置建议等内容。

附件 4

互联网暴露面信息（模板）

一、办公网互联网出入口情况

序号	责任主体	资产名称	资产类型	IP 地址	可访问的网络和系统	其他
1						
2						

二、虚拟专用网络（VPN）出入口情况

序号	责任主体	资产名称	资产类型	IP 地址	软件类型、版本	用途描述	可访问的网络和系统	其他
1								
2								

三、零信任网络出入口情况

序号	责任主体	资产名称	资产类型	IP 地址	软件类型、版本	用途描述	可访问的网络和系统	其他
1								
2								

附件 5

（运行单位）安全防护工作报告（模板）

一、已开展工作及成效

运行单位部署开展网络安全防护工作的总体情况。包括但不限于以下内容:

一是定级备案工作开展情况。包括信息通信网络单元划分、定级备案、资产纳管情况的梳理。

如：对照新修订的《电信网和互联网网络安全防护定级备案实施指南》，系统梳理本单位全部已正式投入运行的X个信息通信网络单元，核查各信息通信网络单元的定级备案信息、资产信息。本单位共有定级备案信息通信网络单元XX个，其中，XX个三级及以上网络单元，XX个二级网络单元，目前所有网络单元已在通信网络安全防护管理系统中备案/XX个系统已在通信网络安全防护管理系统中备案，其他XXX个，因为.....等情况暂未备案。本单位已于X月通过通信网络安全防护管理系统完成定级备案信息、资产信息的更新工作。

二是符合性评测工作开展情况。包括各信息通信网络单元对照相应网络安全防护系列标准防护要求、检测要求，开

展符合性评测的情况。

三是安全风险评估工作开展情况。包括各信息通信网络单元对照 YD/T 1730-2024《电信网和互联网安全风险评估规范》等要求开展安全风险评估的情况。

四是互联网暴露面管理情况。包括互联网暴露面的组织梳理情况，互联网暴露面的整体情况及其安全防护情况（互联网暴露面信息列表作为附件同步提交）。

五是应急预案及演练工作开展情况。包括本单位网络安全应急预案制修订情况，开展网络安全时间应急演练情况、网络安全事件报告情况，以及近三年是否发生重大及以上网络安全事件。

二、发现问题及整改情况

运行单位在开展网络安全防护工作过程中发现的问题与不足，深挖问题隐患成因，提出整改措施，及时消除问题隐患。

三、下一步保护工作方案

运行单位在现有安全保护措施的基础上，全面梳理分析安全保护需求，结合实际制定本单位下一步网络安全防护工作方案，认真开展网络安全建设和整改加固，全面落实安全保护管理和技术措施。