中共常州市委网络安全和信息化领导小组办公室

常网办发〔2016〕1号

关于开展关键信息基础设施网络安全检查的通　　知

各辖市、区委宣传部，市各有关部门和单位，市各有关重点企业：

为贯彻落实习近平总书记关于做好网络安全工作的重要指示精神，根据中央网信办统一部署和省委网信办《关于开展关键信息基础设施网络安全检查的通知》（苏网办发〔2016〕17号）要求，结合我市实际，即日起开展全市关键信息基础设施网络安全检查工作。现将有关事项通知如下。

一、检查内容

（一）关键信息基础设施的数量、分布情况、主管单位、网络安全管理机构、运维机构以及联系方式等。

关键信息基础设施是指面向公众提供网络信息服务或支撑能源、通信、金融、交通、公用事业等重要行业运行的信息系统或工业控制系统。这些系统一旦发生网络安全事故，会影响重要行业正常运行，对政治、经济、科技、社会、文化、国防、环境以及人民生命财产造成严重损失。关键信息基础设施具体确定方法参见《关键信息基础设施确定指南》（附件1）。

（二）关键信息基础设施的主要功能、服务范围、数据存储情况以及遭到破坏后的危害性等。

（三）关键信息基础设施的运行环境、运维方式、网络安全管理和防护情况等。

二、组织方式

（一）我市关键信息基础设施网络安全检查工作在市委网络安全和信息化领导小组统一领导下开展。市委宣传部、市经信委、市公安局、市国安局、市保密局、市委机要局、市通信行业管理办公室、市电子政务中心等职能部门，统筹组织网络安全检查工作。

（二）各辖市区委宣传部统筹组织辖区内各党政机关、企事业单位的关键信息基础设施网络安全检查工作。市各行业主管部门牵头指导本行业按照全市统一部署开展本次网络安全检查工作。

（三）省级部门、人民团体及其直属机构在我市主管、建设的关键信息基础设施，由省级部门、人民团体负责检查，不列入我市检查范围。

三、职责分工

纳入信息安全等级保护的关键信息基础设施网络安全检查工作由市公安局牵头负责；重点工业企业的关键信息基础设施网络安全检查工作由市经信委牵头负责；常州电信、移动、联通等通信运营企业网络安全检查工作由市通信行业管理办公室牵头负责；市政府网站群安全检查工作由市电子政务中心牵头负责；电力、石油石化、煤炭等能源关键信息基础设施网络安全检查工作由市发改委牵头负责；银行、证券、保险等金融关键信息基础设施网络安全检查工作由人行常州分行、市金融办牵头负责；铁路、公路、水运、民航交通关键信息基础设施网络安全检查工作由市交通运输局牵头负责；水利关键信息基础设施网络安全检查工作由市水利局牵头负责；医疗卫生关键信息基础设施网络安全检查工作由市卫计委牵头负责；教育关键信息基础设施网络安全检查工作由市教育局牵头负责；环境保护关键信息基础设施网络安全检查工作由市环保局牵头负责；水、暖、气供应管理、城市轨道交通、污水处理等市政关键信息基础设施网络安全检查工作由市城乡建设局牵头负责；广播、电视播出管控等广播电视关键信息基础设施网络安全检查工作由市文广新局牵头负责。

四、结果报送

（一）省委网信办提供统一的填报工具。填报工具以及使用手册需加QQ群（基础设施工作动员 574272904）进行下载，填报工具使用说明见《填报工具使用手册》。各地、各部门在工具

上填报《2016年关键信息基础设施情况登记表》(附件2),形成关键信息基础设施基本数据。一个单位或部门建设、管理多个关键信息基础设施的,每个关键信息基础设施单独填报一次。最后,在填报工具中点击“生成上报文件”按钮,将生成的“江苏省**单位上报数据.zip”文件,以光盘刻录形式进行报送。

(二)各辖市区委宣传部负责收集辖区内的关键信息基础设施基本数据。汇总后,以光盘刻录形式报送市委宣传部。

(三)各牵头单位负责收集各自职责分工范围内的关键信息基础设施基本数据。各牵头单位汇总后,以光盘刻录形式报送市委宣传部。其中,纳入市政府网站群管理的网站,由各单位根据市电子政务中心提供的公共模板各自填写其余部分,以光盘刻录形式报送市公安局。

(四)如果填报的关键信息基础设施为工控系统,填写《2016年关键信息基础设施情况登记表》表格中“设施名称”时,以“设施名称(工控)”形式标注,并在填写“基本信息—功能描述”时,说明SCADA、DCS或PLC的使用情况和台套数。

五、进度安排

(一)动员部署阶段(8月)

根据省委网信办统一部署,建立网络安全检查职能部门工作联络机制,细化工作方案,组织动员部署。

(二)自查报送阶段(9月)

各地、各部门梳理本地、本部门关键信息基础设施,填报

《2016年关键信息基础设施情况登记表》，并于9月30日前，按照文件要求刻录光盘报送。

各地、各部门要加强对本次检查梳理出的关键信息基础设施的网络安全防护，适时开展网络安全自查，确保运行正常有序。

（三）上报数据和抽查整改阶段（10月-11月）

10月13日前，市委宣传部将统一向上级报送我市关键信息基础设施有关数据。同时，将会同市经信委、市公安局、市国家安全局、市行管办等部门，组织技术力量就各自牵头负责的关键信息基础设施，以远程渗透或现场检查等方式进行抽查。

省委网信办将会同省有关部门，组织技术力量以远程渗透的方式对各地、各部门关键信息基础设施进行技术检测。对发现问题的地方或部门关键信息基础设施，将以问题为导向进行现场核查。主要核实：关键信息基础设施确定和信息填报情况，是否存在应定未定的情况；网络安全自查和隐患整改情况，进一步查找风险隐患；对自查不认真或者风险隐患突出的单位督促其整改。

（四）总结阶段（12月）

汇总形成全市关键信息基础设施清单，总结评估网络安全检查和整改落实情况，并形成书面材料向上报送。

六、工作要求

（一）各地、各部门要高度重视，将本次检查工作列入重要议事日程，落实专人专门负责，明确工作要求、时间节点和工作方式，精心组织实施。

（二）各地、各部门要密切配合，加强工作协同和信息沟通。检查过程中要改变传统的合规检查思路，以发现网络安全风险隐患为主要目标，要强化风险控制，避免检查工作影响关键信息基础设施的正常运行。要加强保密管理，检查结果严格按照规定报送，不得擅自传播至互联网、对外发布或提供给无关机构。

（三）检查工作不得向被检单位收取费用，不得要求被检单位购买、使用指定的产品和服务。

（四）涉及国家秘密的关键信息基础设施不在此次检查范围内，按照国家保密管理规定执行。

报送单位地址及联系人：

市委宣传部：

网络新闻处

地　址：常州市行政中心一号楼A座2216，电话85680816

联系人：陆　炜

市经信委：

信息资源与安全处

地　址：常州市行政中心1号楼B座2214，电话：85681279

联系人：戴国俊

市公安局：

地　址：青果巷188号，常州公安局网络安全保卫支队，电话：81993568

联系人：滕　崴

市国家安全局：

联系人：陈培俊　13775116058

市保密局：

联系人：陈俊峰　85680966

市委机要局：

联系人：杨建军　85680060

市通信行业管理办公室：

地　址：常州市新北区龙锦路1268号14楼

电　话：85686202　　18900653391

联系人：吴亦斌

市电子政务中心：

地　址：市行政中心三号楼B座115，电话：85685015

联系人：韩　波

附件：1. 关键信息基础设施确定指南

2. 关键信息基础设施登记表

中共常州市委网络安全和信息化领导小组办公室

2016年9月2日

附件 1

关键信息基础设施确定指南

（试　行）

一、什么是关键信息基础设施

关键信息基础设施是指面向公众提供网络信息服务或支撑能源、通信、金融、交通、公用事业等重要行业运行的信息系统或工业控制系统，且这些系统一旦发生网络安全事故，会影响重要行业正常运行，对国家政治、经济、科技、社会、文化、国防、环境以及人民生命财产造成严重损失。

关键信息基础设施包括**网站类**，如党政机关网站、企事业单位网站、新闻网站等；**平台类**，如网上购物、网上支付、旅游、论坛、地图、音视频等网络服务平台以及各类智慧应用平台；**生产业务类**，如办公和业务系统、工业控制系统、大型数据中心、云计算平台、电视转播系统等。

二、如何确定关键信息基础设施

关键信息基础设施的确定，通常包括三个步骤，一是确定关键业务，二是确定支撑关键业务的信息系统或工业控制系统，三是根据关键业务对信息系统或工业控制系统的依赖程度，以及信息系统发生网络安全事件后可能造成的损失认定关键信息基础设施。

（一）确定本地区、本部门、本行业的关键业务

可参考下表，结合本地区、本部门、本行业实际梳理关键业务。

行　业		关键业务
能　源	电　力	● 电力生产（含火电、水电、核电等） ● 电力传输 ● 电力配送
	石油石化	● 油气开采 ● 炼化加工 ● 油气输送 ● 油气储存
	煤　炭	● 煤炭开采 ● 煤化工
金　融		● 银行运营 ● 证券期货交易 ● 清算支付 ● 保险运营
交　通	铁　路	● 客运服务 ● 货运服务 ● 运输生产 ● 车站运行
	民　航	● 空运交通管控 ● 机场运行 ● 订票、离港及飞行调度检查安排 ● 航空公司运营
	公　路	● 公路交通管控 ● 智能交通系统（一卡通、ETC 收费等）
	水　运	● 水运公司运营（含客运、货运） ● 港口管理运营 ● 航运交通管控
水　利		● 水利枢纽运行及管控 ● 长距离输水管控 ● 城市水源地管控
医疗卫生		● 医院等卫生机构运行 ● 疾病控制 ● 急救中心运行
环境保护		● 环境监测及预警（水、空气、土壤、核辐射等）
工业制造 （原材料、装备、消费品、电子制造）		● 企业运营管理 ● 智能制造系统（工业互联网、物联网、智能装备等） ● 危化品生产加工和存储管控（化学、核等） ● 高风险工业设施运行管控
市　政		● 水、暖、气供应管理 ● 城市轨道交通 ● 污水处理 ● 智慧城市运行及管控
电信与互联网		● 语音、数据、互联网基础网络及枢纽 ● 域名解析服务和国家顶级域注册管理 ● 数据中心/云服务
广播电视		● 电视播出管控 ● 广播播出管控
政府部门		● 信息公开 ● 面向公众服务 ● 办公业务系统

（二）确定关键业务相关的信息系统或工业控制系统

根据关键业务，逐一梳理出支撑关键业务运行或与关键业务相关的信息系统或工业控制系统，形成候选关键信息基础设施清单。如电力行业火电企业的发电机组控制系统、管理信息系统等；市政供水相关的水厂生产控制系统、供水管网监控系统等。

（三）认定关键信息基础设施

对候选关键信息基础设施清单中的信息系统或工业控制系统，根据本地区、本部门、本行业实际，参照以下标准认定关键信息基础设施。

A. 网站类

符合以下条件之一的，可认定为关键信息基础设施：

1. 县级（含）以上党政机关网站。

2. 重点新闻网站。

3. 日均访问量超过100万人次的网站。

4. 一旦发生网络安全事故，可能造成以下影响之一的：

（1）影响超过100万人工作、生活；

（2）影响单个地市级行政区30%以上人口的工作、生活；

（3）造成超过100万人个人信息泄露；

（4）造成大量机构、企业敏感信息泄露；

（5）造成大量地理、人口、资源等国家基础数据泄露；

（6）严重损害政府形象、社会秩序，或危害国家安全。

5. 其他应该认定为关键信息基础设施。

B. 平台类

符合以下条件之一的，可认定为关键信息基础设施：

1. 注册用户数超过1000万，或活跃用户（每日至少登陆一次）数超过100万。

2. 日均成交订单额或交易额超过1000万元。

3. 一旦发生网络安全事故，可能造成以下影响之一的：

（1）造成1000万元以上的直接经济损失；

（2）直接影响超过1000万人工作、生活；

（3）造成超过100万人个人信息泄露；

（4）造成大量机构、企业敏感信息泄露；

（5）造成大量地理、人口、资源等国家基础数据泄露；

（6）严重损害社会和经济秩序，或危害国家安全。

4. 其他应该认定为关键信息基础设施。

C. 生产业务类

符合以下条件之一的，可认定为关键信息基础设施：

1. 地市级（含）以上政府机关面向公众服务的业务系统，或与医疗、安防、消防、应急指挥、生产调度、交通指挥等相关的城市管理系统。

2. 规模超过1500个标准机架的数据中心。

3. 一旦发生安全事故，可能造成以下影响之一的：

（1）影响单个地市级行政区30%以上人口的工作、生活；

（2）影响10万人用水、用电、用气、用油、取暖或交通出行等；

（3）导致5人以上死亡或50人以上重伤；

（4）直接造成5000万元以上经济损失；

（5）造成超过100万人个人信息泄露；

（6）造成大量机构、企业敏感信息泄露；

（7）造成大量地理、人口、资源等国家基础数据泄露；

（8）严重损害社会和经济秩序，或危害国家安全。

4. 其他应该认定为关键信息基础设施。

附件 2

2016 年关键信息基础设施情况登记表

填表单位（盖章）：

<table>
<tr><td colspan="3">设施名称(全称)：</td></tr>
<tr><td rowspan="5">主管单位信息</td><td>单位全称</td><td></td></tr>
<tr><td>组织机构代码</td><td></td></tr>
<tr><td>单位地址</td><td>省（自治区、直辖市）地（区、市、州、盟）县（区、市、旗）
邮政编码：　　行政区划代码[1]：</td></tr>
<tr><td>单位类型</td><td>☐党政机关　　☐事业单位
☐社会团体　　☐国有及国有控股企业
☐民营企业　　☐其它：</td></tr>
<tr><td>法人代表/单位主要负责人[2]</td><td>姓名：　　职　　务：
固定电话：</td></tr>
<tr><td rowspan="3">联系方式</td><td>上一级主管单位</td><td>☐无
☐有　　主管单位全称：</td></tr>
<tr><td>设施主要负责人</td><td>姓名：　　职　　务：
手机：　固定电话：</td></tr>
<tr><td>网络安全管理部门及负责人</td><td>是否已明确网络安全管理部门：☐是　　☐否
负 责 人：职　　务：
手　　机：　固定电话：</td></tr>
<tr><td>运维单位及联系人</td><td>运维单位全称：
运维联系人：　　手　　机：</td></tr>
</table>

[1]按照《中华人民共和国行政区划代码》（GB/T 2260-2007）规定填写。

[2]无法人代表的单位可填写单位主要负责人。

运行维护	运维模式	□自行运维 □外包运维 主要运维厂商全称：境内厂商 境外厂商 运维方式：　□现场运维　□远程运维
网络安全状况	设施风险评估[9]	对国外产品和服务的依赖程度：　□高　□中　□低 面临的网络安全威胁程度：　□高　□中　□低 网络安全防护能力：　□高　□中　□低
	安全漏洞管理	定期对系统漏洞进行检查分析：□是　□否
	网络安全监测	□无 □自主监测 □委托第三方监测，监测机构全称：

[9]评估方法：

一、对国外产品和服务的依赖程度

1. 高：国外停止产品更新升级、终止技术支持等服务后，关键信息基础设施无法运行。

2. 中：国外停止产品更新升级、终止技术支持等服务后，关键信息基础设施能够运行，但功能、性能等受较大影响。

3. 低：国外停止产品更新升级、终止技术支持等服务后，关键信息基础设施能够正常运转或受影响较小。

二、面临的网络安全威胁程度

1.关键信息基础设施具有下述特征之一的，为高安全威胁：

（1）连接互联网，采用远程在线方式进行运维或对国外产品和服务高度依赖；

（2）跨地区联网运行或网络规模大、用户多，采用远程在线方式进行运维或对国外产品和服务高度依赖；

（3）存在其他可能导致设施中断或运行受严重影响、大量敏感信息泄露等威胁。

2.具有下述特征之一的，为中安全威胁：

（1）连接互联网，对国外产品和服务中度依赖；

（2）跨地区联网运行或网络规模大、用户多，对国外产品和服务中度依赖；

（3）存在其他可能导致设施运行受较大影响、敏感信息泄露等威胁。

3.具有下述特征之一的，为低安全威胁：

（1）连接互联网，对国外产品和服务依赖度低；

（2）跨地区联网运行或网络规模大、用户多，对国外产品和服务依赖度低；

（3）存在其他可能导致设施运行受影响、信息泄露等威胁。

三、网络安全防护能力

1.高：经组织专业技术力量进行攻击测试，不能通过互联网进入或控制设施。

2.中：经组织专业技术力量进行攻击测试，能够通过互联网进入或控制设施，但进入或控制系统的难度较高。

3.低：经组织专业技术力量进行攻击测试，能够轻易通过互联网进入或控制设施。

	云防护措施	□采用云防护服务，服务商全称： □未采用云防护服务
	应急措施	网络安全应急预案：□已制定□未制定 网络安全应急演练：□本年度已开展□本年度未开展
网络安全状况	灾备情况	（可多选） □数据灾备　RPO[10]： □系统灾备 RTO[11]： □无灾备措施
	网络安全事件	2015 年发生的网络安全事件次数：次， 其中由于软硬件故障导致的事件次数：次 2015 年检测发现的高危漏洞数：个
商用密码使用情况	用途	□身份认证□访问控制□电子签名□传输保护 □存储保护□密钥管理□安全审计□其他
	密码设备	□使用了（台套）密码设备 其中，取得国家密码管理局审批型号的数量（台套） 未取得审批型号的国内产品数量（台套） 国外产品数量（台套） □未使用密码设备

[10]RPO（Recovery Point Objective）是指灾难发生后，容灾系统能把数据恢复到灾难发生前时间点的数据，是衡量灾难发生后会丢失多少生产数据的指标。可简单的描述为设施能容忍的最大数据丢失量。

[11]RTO（Recovery Time Objective）则是指灾难发生后，从关键信息基础设施宕机导致业务停顿之刻开始，到业务恢复运营所需要的时间间隔。可简单的描述为设施能容忍的恢复时间。

中共常州市委网络安全和信息化领导小组办公室　2016年9月2日印发