资料 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**，如即时通信、网上购物、网上支付、搜索引擎、电子邮件、论坛、地图、音视频等网络服务平台；**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。

资料 2

关键信息基础设施登记表

填表单位（盖章）：

设施名称（全称）：_____		
主管单位信息	单位全称	
	组织机构代码	
	单位地址	_____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]：_____
	单位类型	☐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：_____
	法人代表/单位主要负责人[2]	姓　　名：_____ 职　　务：_____ 固定电话：_____
	上一级主管单位	☐无 ☐有　　主管单位全称：_____
联系方式	设施主要负责人	姓名：_____ 职　　务：_____ 手机：_____ 固定电话：_____
	网络安全管理部门及负责人	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：_____
	运维单位及联系人	运维单位全称：_____ 运维联系人：_____ 手　　机：_____

[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。

基本信息	设施类型[3]	☐网站类，日均访问量：_____万次 ☐党政机关网站　☐新闻信息网站 ☐事业单位网站　☐社会团体网站 ☐国有企业网站　☐其他：_____ ☐平台类，注册用户数[4]：_____万人 ☐即时通信 ☐网络购物，日均成交订单额：_____万元 ☐网络交易，日均交易额：_____万元 ☐网络支付，日均交易额：_____万元 ☐其他，平台类型：_____ ☐生产业务类 ☐与危险品的生产、运输、仓储等直接关联
	功能描述	（描述该设施所承载的主要功能，服务范围，以及设施对关键业务的支撑作用。）
	网页入口信息[5]	域名：_____ IP 地址：_____ ICP 备案号：_____
	设施特征	是否实时运行：☐是　☐否 是否面向社会公众提供服务：☐是　☐否
	影响分析	发生网络安全事故，可能导致以下后果（可多选）： ☐影响单个地市级行政区 30%以上人口的工作、生活； ☐直接影响 1000 万人工作、生活； ☐影响 10 万人用水、用电、用气、用油、取暖或交通出行等； ☐导致 5 人以上死亡或 50 人以上重伤；

[3]根据附件 1 的《关键信息基础设施确定指南》的分类原则进行确定。
[4]不需要用户注册的平台直接填“0”。
[5]网站和平台类填写网址；生产业务类填写用户登录入口信息；无用户登录入口，可填写后台管理系统登录入口信息。如无域名、ICP 备案号，可不填写。

基本信息	影响分析	☐造成 1000 万元以上直接经济损失； ☐造成超过 100 万人个人信息泄露； ☐造成大量机构、企业敏感信息泄露； ☐造成大量地理、人口、资源等国家基础数据[6]泄露； ☐严重损害社会和经济秩序，或危害国家安全。 ☐其他，影响程度描述：_____
	投入情况	2015 年信息化建设（含运维）总投入（万元）：_____， 其中网络安全总投入（万元）：_____
	信息技术产品国产化率	服务器　数量：_____台　国产化率：_____ 存储设备　数量：_____台　国产化率：_____ 路由器　数量：_____台　国产化率：_____ 交换机　数量：_____台　国产化率：_____ 服务器操作系统　数量：_____套　国产化率：_____ 数据库管理系统　数量：_____套　国产化率：_____
数据存储	数据内容	（可多选） ☐收集或存储个人信息，涉及____万人 ☐收集或存储商业数据，涉及____个机构 ☐收集或存储国家基础数据，涉及数据内容_____
	存储位置	☐全部境内存储　☐有数据境外存储，主要存储地[7]_____
	数据集中	☐全国数据集中　☐省级数据集中　☐无数据集中
	与境外信息系统数据交换	☐存在　☐不存在
	数据加密	☐数据存储与传输均加密　☐数据存储与传输均未加密 ☐仅数据存储加密　☐仅数据传输加密

[6]指人口信息资源、法人单位信息资源、自然资源和空间地理信息资源、电子证照信息资源、社会信用信息资源等国家基础性信息资源。

[7]填写存储地国际长途区号，如美国为 001，日本为 0081

运行环境	网络运行环境	☐与互联网物理隔离 ☐与互联网连接，互联网接入口数量：_____ 个
	托管情况	☐未托管 ☐托　管 主要托管地[8]：_____ 托管单位（全称）：_____ 托管方式：☐主机托管　☐虚拟主机/云计算　☐其它_____
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

[8]如在国内，填写行政区划编码，加在国外，填写所在国国际长途区号，如美国为 001，日本为 0081。

	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：_____
	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
	灾备情况	（可多选）

[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。

网络安全状况		☐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
网络安全状况		
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。

资料 3

网络安全自查表

一、单位基本情况			
单位名称		组织机构代码	
网络安全专职工作人员	①本单位网络安全专职工作人员总数：_____ ②网络安全专职工作人员缺口：_____		
二、信息系统基本情况			
信息系统数量	①信息系统总数（包括本单位自行运维和委托其他单位运维的信息系统）： _____个 其中：网站数：_____ 业务系统数：_____ 办公系统数（含邮件系统）：_____ ②本年度新投入运行信息系统数量：_____个		
互联网接入	①互联网接入口总数：_____ □接入中国联通　接入口数量：_____ □接入中国电信　接入口数量：_____ □其他：_____接入口数量：_____		
门户网站	①域名：_____ .cn 域名 NS 记录：_____ .cn 域名 A 记录：_____ ②IP 地址段：_____ ③主要协议/端口：_____ ④接入运营商：_____接入带宽：_____ ⑤CDN 提供商：_____		
三、网络安全责任制落实情况			
负责网络安全管理工作的单位领导	①负责网络安全管理工作的单位领导：□已明确　□未明确 ②姓名：_____ ③职务：_____ ④是否本单位主要负责同志：□是　□否		
负责网络安全管理工作的内设机构 负责网络安全	①负责网络安全管理工作的内设机构：□已明确　□未明确 ②机构名称：_____ ③负责人：_____职　务：_____		

管理工作的内设机构	④联系人：_____办公电话：_____ 移动电话：_____
网络安全责任制度建设和落实情况	①网络安全责任制度：☐已建立　☐未建立 ②网络安全检查责任：☐已明确　☐未明确 ③本年度网络安全检查专项经费：☐已落实，_____万　☐无专项经费
四、网络安全日常管理情况	
人员管理	①重点岗位人员安全保密协议：☐全部签订　☐部分签订　☐均未签订 ②人员离岗离职安全管理规定：☐已制定　☐未制定 ③外部人员访问机房等重要区域审批制度：☐已建立　☐未建立
信息资产管理	①信息资产管理制度：☐已建立　☐未建立 ②设备维修维护和报废管理： ☐已建立管理制度，且记录完整 ☐已建立管理制度，但记录不完整 ☐未建立管理制度
经费保障	①上一年度信息化总投入：_____万元，网络安全实际投入：_____万元，其中采购网络安全服务比例：_____ ②本年度信息化总预算（含网络安全预算）：_____万元，网络安全预算：_____万元，其中采购网络安全服务比例：_____
五、网络安全防护情况	
网络边界安全防护	①网络安全防护设备部署（可多选）： ☐防火墙　☐入侵检测设备　☐安全审计设备 ☐防病毒网关　☐抗拒绝服务攻击设备　☐Web 应用防火墙 ☐其它 ②设备安全策略配置：☐使用默认配置　☐根据需要配置 ③网络访问日志：☐留存日志　☐未留存日志
无线网络安全防护	①本单位使用无线路由器数量：_____ ②无线路由器用途： ☐访问互联网：_____个 ☐访问业务/办公网络：_____个 ③安全防护策略（可多选）：

无线网络安全防护	☐采取身份鉴别措施　☐采取地址过滤措施 ☐未设置安全防护策略 ④无线路由器使用默认管理地址情况：☐存在　☐不存在 ⑤无线路由器使用默认管理口令情况：☐存在　☐不存在
电子邮件安全防护	①建设方式：☐自行建设 ☐由上级单位统一管理 ☐使用第三方服务　邮件服务提供商_____ ②帐户数量：_____个 ③注册管理：☐须经审批登记　☐任意注册 ④注销管理：☐人员离职后，及时注销　☐无管理措施 ⑤口令管理：☐使用技术措施控制口令强度 位数要求：☐4 位　☐6 位　☐8 位　其他：_____ 复杂度要求：☐数字　☐字母　☐特殊字符 更换频次要求：☐强制定期更换，更换频次：_____ ☐无强制更换要求 ☐没有采取技术措施控制口令强度 ⑥安全防护：（可多选） ☐采取数字证书 ☐采取反垃圾邮件措施 ☐其他：_____
终端计算机安全防护	①管理方式： ☐集中统一管理（可多选） ☐规范软硬件安装　☐统一补丁升级　☐统一病毒防护 ☐统一安全审计　☐对移动存储介质接入实施控制 ☐统一身份管理 ☐分散管理 ②接入互联网安全控制措施： ☐有控制措施（如实名接入、绑定计算机 IP 和 MAC 地址等） ☐无控制措施

<table>
<tr><td>终端计算机安全防护</td><td>③接入办公系统安全控制措施：
☐有控制措施（如实名接入、绑定计算机 IP 和 MAC 地址等）
☐无控制措施</td></tr>
<tr><td>移动存储介质安全防护</td><td>①管理方式：
☐集中管理，统一登记、配发、收回、维修、报废、销毁
☐未采取集中管理方式
②信息销毁：
☐已配备信息消除和销毁设备　☐未配备信息消除和销毁设备</td></tr>
<tr><td>漏洞修复情况</td><td>①漏洞检测周期：☐每月　☐每季度　☐每年　☐不进行漏洞检测
②2015 年自行发现漏洞数量：_____个
收到漏洞风险通报数量：_____个
其中已得到处置的漏洞风险数量：_____个</td></tr>
<tr><td colspan="2">六、网络安全应急工作情况</td></tr>
<tr><td rowspan="2">应急预案</td><td>☐已制定　2015 年修订情况：☐修订　☐未修订
☐未制定</td></tr>
<tr><td>2015 年应急预案启动次数：_____</td></tr>
<tr><td>应急演练</td><td>☐2015 年已开展，演练次数：_____，其中实战演练数：_____
☐2015 年未开展</td></tr>
<tr><td>应急技术队伍</td><td>☐本部门所属　☐外部服务机构　☐无</td></tr>
<tr><td colspan="2">七、网络安全教育培训情况</td></tr>
<tr><td>培训次数</td><td>2015 年开展网络安全教育培训（非保密培训）的次数：_____</td></tr>
<tr><td>培训人数</td><td>2015 年参加网络安全教育培训的人数：_____
占本单位总人数的比例：_____%</td></tr>
<tr><td colspan="2">八、技术产品使用情况</td></tr>
<tr><td rowspan="3">服务器</td><td colspan="8"><table><tr><td>品牌</td><td>联想</td><td>曙光</td><td>浪潮</td><td>华为</td><td>IBM</td><td>HP</td><td>DELL</td><td>Oracle</td></tr><tr><td>数量</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr></table></td></tr>
<tr><td colspan="8">其他：
1. 品牌_____，数量_____</td></tr>
</table>

<table>
<tr><td>服务器</td><td>2. 品牌_____，数量_____
①使用国产 CPU 的台数：_____
②使用国产操作系统的台数：_____</td></tr>
<tr><td>终端计算机
（含笔记本）</td><td><table><tr><td>品牌</td><td>联想</td><td>长城</td><td>方正</td><td>清华同方</td><td>华硕</td><td>宏基</td></tr><tr><td>数量</td><td></td><td></td><td></td><td></td><td></td><td></td></tr></table>其他：
1. 品牌_____，数量_____
2. 品牌_____，数量_____
①使用国产 CPU 的台数：_____
②使用国产操作系统的台数：_____
使用 Windows XP/7/8 的台数：_____
③安装国产字处理软件的台数：_____
④安装国产防病毒软件的台数：_____</td></tr>
<tr><td>数据库
管理系统</td><td><table><tr><td>品牌</td><td>金仓</td><td>达梦</td><td>Oracle</td><td>DB2</td><td>SQLServer</td><td>Access</td><td>MySQL</td></tr><tr><td>数量</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr></table>其他：
1. 品牌_____，数量_____
2. 品牌_____，数量_____</td></tr>
<tr><td>路由器</td><td><table><tr><td>品牌</td><td>华为</td><td>中兴</td><td>锐捷网络</td><td>H3C</td><td>Cisco</td><td>Juniper</td></tr><tr><td>数量</td><td></td><td></td><td></td><td></td><td></td><td></td></tr></table>其他：
1. 品牌_____，数量_____
2. 品牌_____，数量_____</td></tr>
<tr><td>交换机</td><td><table><tr><td>品牌</td><td>华为</td><td>中兴</td><td>锐捷网络</td><td>H3C</td><td>Cisco</td><td>Juniper</td></tr><tr><td>数量</td><td></td><td></td><td></td><td></td><td></td><td></td></tr></table>其他：
1. 品牌_____，数量_____
2. 品牌_____，数量_____</td></tr>
<tr><td>存储设备</td><td>总台数：_____</td></tr>
</table>

	品牌：_____ 数量：_____ 品牌：_____ 数量：_____
邮件系统	总数：_____ 品牌：_____ 数量：_____ 品牌：_____ 数量：_____

九、商用密码使用情况

①密码功能用途（可多选）：

☐身份认证 ☐访问控制 ☐电子签名 ☐安全审计

☐传输保护 ☐存储保护 ☐密钥管理

②密码机 数量：_____ 密码系统 数量：_____

智能 IC 卡 数量：_____ 智能密码钥匙 数量：_____

动态令牌 数量：_____

③所采用的密码算法：

对称算法：☐SM1 ☐SM4 ☐SM7 ☐AES ☐DES ☐3DES

非对称算法：☐SM2 ☐SM9 ☐RSA1024 ☐RSA2048

杂凑算法：☐SM3 ☐SHA-1 ☐SHA-256 ☐SHA-384 ☐SHA-512 ☐MD5

其它：_____

十、本年度技术检测及网络安全事件情况

技术检测情况	渗透测试	进行渗透测试的系统数量：_____ 其中，可以成功控制的系统数量：_____
	恶意代码[1]检测	①进行病毒木马等恶意代码检测的服务器台数：_____ 其中，存在恶意代码的服务器台数：_____ ②进行病毒木马等恶意代码检测的终端计算机台数：_____ 其中，存在恶意代码的终端计算机台数：_____

[1]本表所称恶意代码，是指病毒木马等具有避开安全保护措施、窃取他人信息、损害他人计算机及信息系统资源、对他人计算机及信息系统实施远程控制等功能的代码或程序。

技术检测情况	安全漏洞检测结果	①进行漏洞扫描的服务器台数：_____ 其中，存在高风险漏洞[2]的服务器台数：_____ ②进行漏洞扫描的终端计算机台数：_____ 其中，存在高风险漏洞的终端计算机台数：_____
网络安全事件情况		①监测到的网络攻击次数：_____ 其中：本单位遭受 DDoS 攻击次数：_____ 被嵌入恶意代码次数：_____ ②网络安全事件次数：_____ 其中：服务中断次数：_____ 信息泄露次数：_____ 网页被篡改次数：_____

十一、信息技术外包服务机构情况（包括参与技术检测的外部专业机构）

外包服务机构 1	机构名称	
	机构性质	□国有单位　□民营企业 □外资企业　□合资企业
	服务内容	□系统集成　□系统运维　□风险评估 □安全检测　□安全加固　□应急支持 □数据存储　□数据分析　□灾难备份 □安全监测　□流量清洗　□其他
外包服务机构 2	机构名称	
	机构性质	□国有单位　□民营企业 □外资企业　□合资企业
	服务内容	□系统集成　□系统运维　□风险评估 □安全检测　□安全加固　□应急支持 □数据存储　□数据分析　□灾难备份 □安全监测　□流量清洗　□其他

[2]本表所称高风险漏洞，是指计算机硬件、软件或信息系统中存在的严重安全缺陷，利用这些缺陷可完全控制或部分控制计算机及信息系统，对计算机及信息系统实施攻击、破坏、信息窃取等行为。