附件1

关键信息基础设施基础调查流程

一、关键信息基础设施定义

关键信息基础设施是指关系国家核心利益、人民群众生命财产安全和社会生产生活秩序，一旦遭到破坏、丧失功能或数据泄露，可能严重危害国家安全、国计民生和公共利益的网络基础设施、重要业务系统和生产控制系统以及重要数据资源等。

二、关键信息基础设施范围

下列单位或行业运营使用的网络基础设施、重要业务系统和生产控制系统以及重要数据资源等，应当纳入关键信息基础设施，并在开展网络安全等级保护的基础上，实施重点保护。原则上安全保护等级在第三级（含）以上的保护对象才能纳入关键信息基础设施范围。

（一）电信网、广电网、互联网等基础信息网络，以及云计算、大数据和其他大型公共网络服务的运营单位;

（二）能源、资源、金融、交通、公用事业、应急救援、环境保护等为社会生产生活提供基础支撑的重要行业；

（三）国防科工、航空航天、大型装备、核工业、化工、食品药品、信息技术等研制生产单位；

（四）广播电台、电视台、通讯社等新闻单位；

（五）管理国家事务和提供公共服务的国家机关；

（六）其他关系国家核心利益、人民群众生命财产安全和社会生产生活秩序的单位或行业。

三、关键信息基础设施的梳理流程

（一）全面开展调查摸底。各行业、各部门要部署本行业、本部门重要信息系统运营使用单位全面梳理本行业、本部门网络基础设施、重要业务系统和生产控制系统以及重要数据资源底数，根据《网络安全法》和国家关键信息基础设施定义和范围，在网络安全等级保护制度的基础上，结合本行业、本部门第三级（含）以上信息系统在公众服务、经济建设、社会发展等涉及国计民生领域的重要程度以及一旦遭到破坏后的危害程度，初步梳理本行业、本部门国家关键信息基础设施。

（二）组织行业内部评估。各行业主管部门要加强对本行业各重要信息系统运营使用单位如何梳理关键信息基础设施工作的指导，及时汇总本行业各重要信息系统运营使用单位梳理的国家关键信息基础设施名单，组织行业内部专家根据网络基础设施、重要业务系统和生产控制系统以及重要数据资源在本行业的重要程度，结合行业特点逐一进行评估和专家评审，梳理出本行业国家关键信息基础设施。

附件2

行业部门国家关键信息基础设施基础调查表

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **序号** | **单位名称** | **联系人** | **数量** | **关键信息基础设施名称** | **安全保护等级** | **备案编号** | **备案公安机关名称** |
| **姓名** | **电话** |
| 1 | 单位1 |  |  |  | 等级保护备案系统（网络、系统或数据资源等） |  |  |  |
| 等级保护备案系统（网络、系统或数据资源等） |  |  |  |
| ....... |  |  |  |
| 2 | 单位2 |  |  |  | 等级保护备案系统（网络、系统或数据资源等） |  |  |  |
| 等级保护备案系统（网络、系统或数据资源等） |  |  |  |
| ....... |  |  |  |
| **合计** | **单位总数** |  | **关键信息基础设施总 数** |  |

附件3

国家关键信息基础设施基本情况表

|  |  |
| --- | --- |
| 等级保护备案系统（网络、系统或数据资源等） |  |
| 运营使用单位名称 |  |
| 单位联系人姓名 |  | 固定电话 |  |
| 手机电话 |  |
| 安全保护等级 |  | 备案编号 |  |
| 所属行业/领域 |  | 受理备案的公安机关 |  |
| 服务范围 |  | 服务对象 |  |
| 关键信息基础设施是否连接互联网？□是□否（注：如果连接互联网，请填写关键信息基础设施以下接入信息） |
| 域名 |  |
| 域名注册服务机构和联系方式 |  |
| .cn域名的NS记录 |  |
| .cn域名的A记录 |  |
| 主站IP地址范围 |  |
| 主要协议/端口 |  | 操作系统版本 |  |
| 接入运营商及联系方式 |  |
| 物理接入位置 |  |
| 接入带宽 |  |
| CDN IP地址范围 |  |
| CDN 服务提供商 |  |
| CDN 联系人姓名 |  | 手机号 |  |

附件4

2017年重点单位网络安全自查表

表一：行业主管部门填写

|  |
| --- |
| 一、行业主管部门基本情况 |
| 行业主管部门名称 |  |
| 单位地址 |  |
| 网络安全分管领导 | 姓名 |  | 职务/职称 |  |
| 网络安全责任部门 |  |
| 责任部门负责人 | 姓 名 |  | 职务/职称 |  |
| 办公电话 |  | 移动电话 |  |
| 责任部门联系人 | 姓 名 |  | 职务/职称 |  |
| 办公电话 |  | 移动电话 |  |
| 传 真 |  | 邮箱地址 |  |
| 全行业信息系统总数 |  | 第四级系统数 |  | 第三级系统数 |  |
| 第二级系统数 |  | 未定级系统数 |  |
| 全行业信息系统等级测评总数 |  | 第四级系统数 |  | 第三级系统数 |  |
| 第二级系统数 |  | 未测评系统数 |  |
| 全行业信息系统安全建设整改总数 |  | 第四级系统数 |  | 第三级系统数 |  |
| 第二级系统数 |  | 未整改系统数 |  |
| 本级单位信息系统总数 |  | 第四级系统数 |  | 第三级系统数 |  |
| 第二级系统数 |  | 未整改系统数 |  |
| 二、行业主管部门网络安全工作情况 |
| 1、行业网络安全工作的组织领导情况 |
| （重点包括：行业网络安全领导机构或网络安全等级保护工作领导机构成立情况；行业网络安全或网络安全等级保护工作的职责部门和具体职能情况；全行业网络安全等级保护工作部署情况等。） |
| 2、行业网络安全等级保护工作保障情况 |
| （重点包括：行业网络安全等级保护工作年度考核情况；行业主管部门组织对地方对口部门或所属企事业单位网络安全检查情况；行业网络安全工作经费是否纳入年度预算?行业网络安全工作的经费约占行业信息化建设经费的百分比情况等。） |
| 3、行业网络安全责任追究制度执行情况 |
| （重点包括：是否建立了行业网络安全责任追究制度？是否依据责任追究制度对行业发生的网络安全事件（事故）进行追责等情况。） |
| 4、行业网络安全与信息通报工作情况 |
| （重点包括：是否加入了国家网络与信息安全通报机制？是否建立了本行业网络与信息安全通报机制？行业组织开展日常网络安全监测情况；本行业开展网络与信息安全通报预警工作的总体情况等。） |
| 5、行业重要网络安全政策和技术标准的制定情况 |
| （重点包括：行业出台网络安全或等级保护政策、管理办法、管理规定等规范性文件情况，具体文件名字和出台时间；行业出台网络安全或等级保护标准规范情况，具体文件名字和出台时间等情况。） |
| 6、行业网络安全顶层设计和统筹规划情况 |
| （重点包括：行业网络安全顶层设计情况；行业网络安全工作的短期目标和长远规划制定情况；全行业的网络安全保护策略制定情况等。） |
| 7、行业数据资源保护情况 |
| （重点包括：行业数据中心建设情况；行业数据资源存储情况；行业数据资源安全保护情况；行业数据资源的灾备中心建设情况和数据备份恢复情况，行业数据资源存储和应用是否由社会第三方提供？提供服务单位的具体情况等） |
| 8、行业网络安全应急预案和演练情况 |
| （重点包括：是否制定了行业网络安全预案？行业网络安全预案是否进行了演练？是否根据演练情况对预案进行了修改完善等情况） |
| 9、行业网络安全应急队伍建设情况 |
| （重点包括：是否建立了本行业网络安全应急队伍？是否组建了行业网络安全专家队伍？是否与社会企业签订了应急支持协议？行业应急队伍建设规划等情况。） |
| 10、行业网络安全事件（事故）的处置情况 |
| （重点包括：是否明确了行业网络安全事件（事故）发现、报告和处置流程？年内是否发生重大网络安全事件（事故）？是否与相关部门建立了网络安全应急处置机制等情况。） |
| 11、行业网络安全宣传培训情况 |
| （重点包括：行业组织开展网络安全宣传教育情况；行业组织开展网络安全领导干部培训、业务骨干培训和网络安全员培训等情况。）　 |
| 12、行业新技术、新应用安全保护情况 |
| （重点包括：行业大数据、云计算、物联网、工业控制系统等应用情况；是否开展等级保护工作情况；新技术、新应用网络安全保护等情况。） |

表二：信息系统运营使用单位填写

|  |
| --- |
| 一、信息系统运营使用单位基本情况 |
| 单位名称 |  |
| 单位地址 |  |
| 网络安全分管领导 | 姓名 |  | 职务/职称 |  |
| 网络安全责任部门 |  |
| 责任部门负责人 | 姓名 |  | 职务/职称 |  |
| 办公电话 |  | 移动电话 |  |
| 责任部门联系人 | 姓名 |  | 职务/职称 |  |
| 办公电话 |  | 移动电话 |  |
| 单位信息系统总数 |  | 第四级系统数 |  | 第三级系统数 |  |
| 第二级系统数 |  | 未定级系统数 |  |
| 单位信息系统等级测评总数 |  | 第四级系统数 |  | 第三级系统数 |  |
| 第二级系统数 |  | 未测评系统数 |  |
| 单位信息系统安全建设整改总数 |  | 第四级系统数 |  | 第三级系统数 |  |
| 第二级系统数 |  | 未整改系统数 |  |
| 单位信息系统安全自查总数 |  | 第四级系统数 |  | 第三级系统数 |  |
| 第二级系统数 |  | 未自查系统数 |  |
| 二、信息系统运营使用单位网络安全工作情况 |
| 1、单位网络安全等级保护工作的组织领导情况 |
| （重点包括：单位网络安全领导机构或网络安全等级保护工作领导机构成立情况；单位网络安全或网络安全等级保护工作的职责部门和具体职能情况；单位网络安全等级保护工作部署情况等。） |
| 2、单位对网络安全等级保护工作的保障情况 |
| （重点包括：单位网络安全等级保护工作年度考核情况；单位组织开展网络安全自查情况；单位网络安全工作经费是否纳入年度预算?单位网络安全工作的经费约占单位信息化建设经费的百分比情况等。） |
| 3、单位网络安全责任追究制度执行情况 |
| （重点包括：是否建立了单位网络安全责任追究制度？是否依据责任追究制度对单位发生的网络安全事件（事故）进行追责等情况。） |
| 4、单位信息系统定级备案工作情况 |
| （重点包括：单位信息系统是否全部定级备案？单位系统调整是否及时进行备案变更？单位新建信息系统是否落实定级备案等工作。） |
| 5、单位信息系统安全测评和安全建设整改工作情况 |
| （重点包括：单位信息系统安全检测和整改经费落实情况；单位信息系统恶意代码扫描、渗透性测试、等级测评和风险评估的安全检测情况；信息系统安全建设整改方案制定和实施情况；单位网络安全保护状况的了解掌握等情况。） |
| 6、单位网络安全管理制度的制定和实施情况 |
| （重点包括：单位信息系统建设和网络安全“同步规划、同步建设、同步运行”措施的落实情况；单位人员管理，信息系统机房管理、设备管理、介质管理、网络安全建设管理、运维管理、服务外包等管理制度的建设情况；管理制度的监督保障和运行情况等。） |
| 7、单位重要数据的保护情况 |
| （重点包括：单位数据中心建设情况；单位重要数据存储和安全保护情况；单位重要数据备份恢复情况，单位重要数据存储和应用是否由社会第三方提供？提供服务单位的具体情况等） |
| 8、单位网络安全监测和预警情况 |
| （重点包括：单位开展日常网络安全监测情况；单位网络安全监测技术手段建设情况；单位网络安全预警工作情况等。） |
| 9、单位网络安全应急预案和演练情况 |
| （重点包括：是否制定了单位网络安全预案？单位网络安全预案是否进行了演练？是否根据演练情况对预案进行了修改完善等情况。） |
| 10、单位网络安全事件（事故）的处置情况 |
| （重点包括：是否明确了单位网络安全事件（事故）发现、报告和处置流程？年内是否发生重大网络安全事件（事故）？是否与相关部门建立了网络安全应急处置机制等情况。） |
| 11、单位信息技术产品、服务国产化情况 |
| （重点包括：单位操作系统、服务器、数据库、交换机等核心信息技术产品的国产化比率情况；单位网络安全设备的国产化比率情况；单位信息技术产品国产化替换工作计划情况；单位新建信息系统是否采用国产化设备；单位信息安全服务情况等。）　 |
| 12、单位网络安全宣传培训情况 |
| （重点包括：单位组织开展网络安全宣传教育情况；单位组织开展网络安全岗位培训和网络安全员培训等情况。） |
| 三、单位信息系统基本情况 |
| 序号 | 信息系统名称 | 是否定级 | 是否备案 | 是否为关键信息基础设施 | 备案编号 | 安全保护等级 |
| 1 |  |  |  |  |  |  |
| 2 |  |  |  |  |  |  |
| 3 |  |  |  |  |  |  |
| 4 |  |  |  |  |  |  |
| ....... |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |

表三：网站安全情况自查表

|  |
| --- |
| 一、网站的基本情况 |
| 网站中文名 | 　 | IP地址 | 　 |
| 网 址 | 　 |
| 网站责任单位 | 　 | 网站运行单位 | 　 |
| 网站责任单位负责人及职务 | 　 | 联系电话 | 　 |
| 网站运行安全责任人及职务 | 　 | 联系电话 | 　 |
| 网站责任单位所在地 | 　 |
| 工信部ICP备案号 | 　 |
| 国际联网备案号 | 　 |
| 隶 属 关 系 | □中央 □省(自治区、直辖市) □地(区、市、州、盟) □县（区、市、旗） □其他\_\_\_\_\_ |
| 单 位 类 型 | □政府机关 □事业单位 □国企□互联网 □其他\_\_\_\_\_ |
| 行业类别 | 如：财政（根据等级保护备案表行业分类划分） |
| 等级保护定级备案 | □二级 □三级 □四级 □未定级 |
| 等 级 测 评 | □已开展 □未开展 |
| 网站安全责任书 | □已签订 □未签订 |
| 网站服务栏目 | □新闻发布 □政策宣传 □事项办理 □论 坛 □即时通信□电子邮件 □留言版 □政务公开 □其他\_\_\_\_\_  |
| 二、网站的联网信息 |
| 域名注册服务机构和联系方式 |  |
| .cn域名的NS记录 |  |
| .cn域名的A记录 |  |
| 主站IP地址范围 |  |
| 主要协议/端口 |  | 操作系统版本 |  |
| 接入运营商及联系方式 |  |
| 物理接入位置 |  |
| 接 入 带 宽 |  |
| CDN IP地址范围 |  |
| CDN 服务提供商 |  |
| CDN 联系人姓名 |  | 手机号 |  |

|  |
| --- |
| 三、网站安全保护情况 |
| 1 | 网站安全责任部门和安全责任人落实情况 | 是否落实了单位网站安全责任部门？ | □是 □否 |
| 是否落实了单位网站安全责任人？ | □是 □否 |
| 2 | 主要领导对网站网络安全工作的重视情况 | 是否将网站安全工作的执行情况纳入到年度考核指标？ | □是 □否  |
| 开展网站安全工作的经费是否纳入年度预算？ | □是 □否  |
| 3 | 单位网站网络安全责任制落实情况 | 是否明确了网站建设单位、运维单位和内容更新单位等部门的责任？ | □是 □否  |
| 是否对发生的网站安全事件（事故）按照安全责任制进行追责？ | □是 □否  |
| 4 | 关键岗位人员配备情况 | 是否有明确的安全管理员，并签订保密协议？ | □是 □否  |
| 是否有内容管理员，并签订保密协议？ | □是 □否  |
| 5 | 网站定级备案执行情况 | 单位网站是否确定了安全保护等级？ | □是 □否  |
| 单位网站是否按要求到公安机关进行了备案？ | □是 □否  |
| 6 | 网站等级测评情况 | 是否从《全国网络安全等级保护测评机构推荐目录》中选择测评机构开展等级测评？ | □是 □否  |
| 是否对网站系统定期进行安全测评？ | □是 □否  |
| 是否对网站系统进行了外部渗透测试？ | □是 □否 |
| 是否根据测评和渗透测试结果对网站进行安全加固改造？  | □是 □否 |
| 7 | 安全事件报告处置 | 是否制定网站安全事件（事故）报告制度？ | □是 □否 |
| 发生网站安全事件（事故）是否向属地公安机关报告？ | □是 □否  |
| 是否有完整网站安全事件处置记录？ | □是 □否 |
| 是否按照要求保留网站完整日志？ | □是 □否  |
| 8 | 开展网站安全监测和预警情况 | 本单位是否开展日常网站安全监测？ | □是 □否  |
| 是否有网站安全监测记录？ | □是 □否  |
| 是否有网站安全预警和处理记录？ | □是 □否  |
| 9 | 网站内容管理 | 是否制定网站内容发布管理制度？ | □是 □否  |
| 是否制定网站内容发布流程？ | □是 □否  |
| 10 | 应急预案的制定、演练和完善情况 | 是否有应急预案，并有相应的预案文档？ | □是 □否  |
| 是否有应急保障队伍并有人员联系方式？ | □是 □否  |
| 是否定期应急演练并有应急演练的文档记录？ | □是 □否  |
| 是否根据演练结果对应急预案进行完善？ | □是 □否  |
| 11 | 机房安全管理制度执行情况 | 本单位机房进出人员管理是否按照制度执行，并有详细记录？ | □是 □否  |
| 本单位机房日常监控是否制度执行并有监控记录？ | □是 □否  |
| 12 | 网络安全检查情况 | 是否有网站安全自查工作总结报告？ | □是 □否  |
| 13 | 网站交互式栏目信息巡查情况 | 单位网站是否有交互式栏目？ | □是 □否  |
| 是否有专人负责网站交互式栏目信息巡查？ | □是 □否  |
| 14 | 网络边界安全防护设备情况 | 是否部署防火墙？ | □是 □否  |
| 是否对外屏蔽了不必要的服务/端口？ | □是 □否  |
| 是否部署入侵检测（防护）设备？ | □是 □否  |
| 是否部署防病毒网关？ | □是 □否  |
| 是否部署抗拒绝服务攻击设备？ | □是 □否  |
| 是否部署Web应用防火墙？ | □是 □否  |
| 是否部署设备？ | □是 □否  |
| 15 | 网页防篡改措施 | 是否定期对网站文件进行检测？ | □是 □否  |
| 是否采取网页防篡改措施？ | □是 □否  |
| 16 | 漏洞扫描措施及修复升级情况 | 是否进行过系统层漏洞扫描，并有详细记录？ | □是 □否  |
| 是否进行过应用层漏洞扫描，并有详细记录？ | □是 □否  |
| 发现的漏洞是否及时修复？ | □是 □否  |
| 17 | 网站恶意代码防护 | 是否有网页挂马检测系统？ | □是 □否  |
| 18 | 网站内容安全防护措施 | 内容编辑、审核及发布权限是否分离？ | □是 □否  |
| 关键信息发布是否多级审核？ | □是 □否  |
| 网站发布内容是否过滤？ | □是 □否  |
| 19 | 管理终端安全防护措施 | 是否有控制措施（如地址绑定，网络接入控制等）？ | □是 □否  |
| 20 | 网站后台管理系统防护措施 | 是否对网站后台管理系统的接口进行隐藏？ | □是 □否  |
| 网站后台管理系统登录是否采取验证机制？ | □是 □否  |
| 是否对网站后台管理系统的登录失败尝试次数进行限制？ | □是 □否  |
| 是否对网站后台管理系统的用户口令复杂度进行强度限制？ | □是 □否  |
| 21 | 主要设备可用性 | 网站服务器和数据库服务器是否双机热备？ | □是 □否  |
| 网站服务器和数据库服务器是否采用冷备方式？ | □是 □否  |
| 22 | 网站前、后台系统隔离情况 | 是否采用逻辑隔离？ | □是 □否  |
| 23 | 网站应用远程管理情况 | 是否不允许远程管理网站的应用？ | □是 □否  |
| 应用远程管理时是否采用加密通道？ | □是 □否  |
| 24 | 网站内容远程维护情况 | 是否不允许远程维护网站内容？ | □是 □否  |
| 网站内容远程维护时是否采用加密通道？ | □是 □否  |
| 25 | 网站服务器操作系统安全措施 | 网站服务器操作系统安全补丁是否及时更新？ | □是 □否  |
| 网站服务器操作系统是否存在弱口令？ | □是 □否  |
| 26 | 网站服务器数据库安全措施 | 网站服务器数据库是否存在弱口令？ | □是 □否  |
| 网站服务器数据库是否共用同一管理口令？ | □是 □否  |
| 27 | 网站服务器中间件安全措施 | 网站服务器中间件管理界面是否允许外部访问？ | □是 □否  |
| 网站服务器中间件是否存在弱口令？ | □是 □否  |
| 28 | 网站安全整治专项工作情况 | 是否完成网站通信管理部门备案？ | □是 □否  |
| 是否完成网站等级保护备案？ | □是 □否 |
| 是否完成网站统一标识？ | □是 □否  |