

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。各单位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。

三、关键信息基础设施的梳理流程

（一）全面开展调查摸底。各单位要全面梳理本单位各部门网络基础设施、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，结合本单位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）组织单位内部评估。各单位责任部门要加强对本单位各重要信息系统运营使用部门如何梳理关键信息基础设施工作的指导，组织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单位的重要

程度，逐一进行评估和专家评审，梳理出本单位关键信息基础设施。

(三) 汇总填表上报。各单位请于 5 月 21 日前 (各厅直属单位请于 5 月 13 日前) 梳理出本单位关键信息基础设施名单，并填报《关键信息基础设施基础调查表》报送省教育厅。每个梳理出的关键信息基础设施要同时填报《关键信息基础设施基本情况表》，连同电子版一并报送。

附件 2

关键信息基础设施基础调查表 (2017.5)

| 单位名称 | 单位联系人 | | 关键信息基础设施总数 | 序号 | 关键信息基础设施名称 | 信息安全等级保护等级 | 省教育厅备案编号 | 公安机关备案编号 | 备案公安机关名称 |
|----------|-------|----|------------|----|-----------------------|------------|----------|----------|----------|
| | 姓名 | 电话 | | | | | | | |
| (加盖单位公章) | | | | | 等级保护备案系统（网络、系统或数据资源等） | 第 级 | | | |
| | | | | | 等级保护备案系统（网络、系统或数据资源等） | 第 级 | | | |
| | | | | | 等级保护备案系统（网络、系统或数据资源等） | 第 级 | | | |
| | | | | | 等级保护备案系统（网络、系统或数据资源等） | 第 级 | | | |
| | | | | | | | | | |

附件 3

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 | | |
| 信息安全等级保护等级 | 省教育厅备案编号 | | |
| 公安机关备案编号 | 受理备案的公安机关 | | |
| 服务范围 | 服务对象 | | |
| <p>关键信息基础设施是否连接互联网？ <input type="checkbox"/>是 <input type="checkbox"/>否</p> <p>（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）</p> | | | |
| 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

网站规范管理工作进展情况表

| | | | |
|------------|---|------------|---|
| 单位名称 | | | |
| 本单位信息系统数量 | | 完成信息发布整改数量 | |
| 完成网站开办审核工作 | <input type="checkbox"/> 是 <input type="checkbox"/> 否 | 完成网站挂标工作 | <input type="checkbox"/> 是 <input type="checkbox"/> 否 |
| 事业单位门户网站数量 | | 完成网站挂标工作数量 | |

附件 5

网络安全自查表

| 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小组成立情况；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、关键信息基础设施的保障、保护情况

| |
|--|
| <p>4、单位网络安全责任追究制度执行情况</p> |
| <p>（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。）</p> |
| <p>5、单位信息系统定级备案工作情况</p> |
| <p>（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。）</p> |
| <p>6、单位信息系统安全测评和安全建设整改工作情况</p> |
| <p>（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。）</p> |
| <p>7、单位网络安全管理制度的制定和实施情况</p> |
| <p>（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。）</p> |

8、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）

9、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。）

10、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。）

11、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。）

12、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。）

13、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。）

| 四、网站安全情况自查情况 | | | |
|--------------|--|--------|--|
| (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 | <input type="checkbox"/> 中央 <input type="checkbox"/> 省(自治区、直辖市) <input type="checkbox"/> 地(区、市、州、盟) <input type="checkbox"/> 县(区、市、旗) <input type="checkbox"/> 其他_____ | | |
| 单位类型 | <input type="checkbox"/> 政府机关 <input type="checkbox"/> 事业单位 <input type="checkbox"/> 国企 <input type="checkbox"/> 互联网 <input type="checkbox"/> 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 | <input type="checkbox"/> 二级 <input type="checkbox"/> 三级 <input type="checkbox"/> 四级 <input type="checkbox"/> 未定级 | | |
| 等级测评 | <input type="checkbox"/> 已开展 <input type="checkbox"/> 未开展 | | |
| 网站安全责任书 | <input type="checkbox"/> 已签订 <input type="checkbox"/> 未签订 | | |
| 网站服务栏目 | <input type="checkbox"/> 新闻发布 <input type="checkbox"/> 政策宣传 <input type="checkbox"/> 事项办理 <input type="checkbox"/> 论坛 <input type="checkbox"/> 即时通信 <input type="checkbox"/> 电子邮件 <input type="checkbox"/> 留言版 <input type="checkbox"/> 政务公开 <input type="checkbox"/> 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责任人落实情况 | 是否落实了单位网站安全责任部门？ | <input type="checkbox"/> 是 <input type="checkbox"/> 否 |
| | | 是否落实了单位网站安全责任人？ | <input type="checkbox"/> 是 <input type="checkbox"/> 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？ | <input type="checkbox"/> 是 <input type="checkbox"/> 否 |
| | | 开展网站安全工作的经费是否纳入年度预算？ | <input type="checkbox"/> 是 <input type="checkbox"/> 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？ | <input type="checkbox"/> 是 <input type="checkbox"/> 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？ | <input type="checkbox"/> 是 <input type="checkbox"/> 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？ | <input type="checkbox"/> 是 <input type="checkbox"/> 否 |
| | | 是否有内容管理员，并签订保密协议？ | <input type="checkbox"/> 是 <input type="checkbox"/> 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？ | <input type="checkbox"/> 是 <input type="checkbox"/> 否 |
| | | 单位网站是否按要求到公安机关进行了备案？ | <input type="checkbox"/> 是 <input type="checkbox"/> 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？ | <input type="checkbox"/> 是 <input type="checkbox"/> 否 |
| | | 是否对网站系统定期进行安全测评？ | <input type="checkbox"/> 是 <input type="checkbox"/> 否 |
| | | 是否对网站系统进行了外部渗透测试？ | <input type="checkbox"/> 是 <input type="checkbox"/> 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？ | <input type="checkbox"/> 是 <input type="checkbox"/> 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？ | <input type="checkbox"/> 是 <input type="checkbox"/> 否 |
| | | 发生网站安全事件（事故）是否向属地公安机关报告？ | <input type="checkbox"/> 是 <input type="checkbox"/> 否 |
| | | 是否有完整网站安全事件处置记录？ | <input type="checkbox"/> 是 <input type="checkbox"/> 否 |
| | | 是否按照要求保留网站完整日志？ | <input type="checkbox"/> 是 <input type="checkbox"/> 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？ | <input type="checkbox"/> 是 <input type="checkbox"/> 否 |
| | | 是否有网站安全监测记录？ | <input type="checkbox"/> 是 <input type="checkbox"/> 否 |
| | | 是否有网站安全预警和处理记录？ | <input type="checkbox"/> 是 <input type="checkbox"/> 否 |
| 9 | 网站内容管理 | 是否制定网站内容发布管理制度？ | <input type="checkbox"/> 是 <input type="checkbox"/> 否 |
| | | 是否制定网站内容发布流程？ | <input type="checkbox"/> 是 <input type="checkbox"/> 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？ | <input type="checkbox"/> 是 <input type="checkbox"/> 否 |
| | | 是否有应急保障队伍并有人员联系方式？ | <input type="checkbox"/> 是 <input type="checkbox"/> 否 |
| | | 是否定期应急演练并有应急演练的文档记录？ | <input type="checkbox"/> 是 <input type="checkbox"/> 否 |
| | | 是否根据演练结果对应急预案进行完善？ | <input type="checkbox"/> 是 <input type="checkbox"/> 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？ | <input type="checkbox"/> 是 <input type="checkbox"/> 否 |
| | | 本单位机房日常监控是否制度执行并有监控记录？ | <input type="checkbox"/> 是 <input type="checkbox"/> 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？ | <input type="checkbox"/> 是 <input type="checkbox"/> 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？ | <input type="checkbox"/> 是 <input type="checkbox"/> 否 |
| | | 是否有专人负责网站交互式栏目信息巡查？ | <input type="checkbox"/> 是 <input type="checkbox"/> 否 |
| 14 | 网络边界安全防护设备情况 | 是否部署防火墙？ | <input type="checkbox"/> 是 <input type="checkbox"/> 否 |
| | | 是否对外屏蔽了不必要的服务/端口？ | <input type="checkbox"/> 是 <input type="checkbox"/> 否 |
| | | 是否部署入侵检测（防护）设备？ | <input type="checkbox"/> 是 <input type="checkbox"/> 否 |
| | | 是否部署防病毒网关？ | <input type="checkbox"/> 是 <input type="checkbox"/> 否 |
| | | 是否部署抗拒绝服务攻击设备？ | <input type="checkbox"/> 是 <input type="checkbox"/> 否 |
| | | 是否部署 Web 应用防火墙？ | <input type="checkbox"/> 是 <input type="checkbox"/> 否 |
| 15 | 网页防篡改措施 | 是否定期对网站文件进行检测？ | <input type="checkbox"/> 是 <input type="checkbox"/> 否 |
| | | 是否采取网页防篡改措施？ | <input type="checkbox"/> 是 <input type="checkbox"/> 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？ | <input type="checkbox"/> 是 <input type="checkbox"/> 否 |
| | | 是否进行过应用层漏洞扫描，并有详细记录？ | <input type="checkbox"/> 是 <input type="checkbox"/> 否 |
| | | 发现的漏洞是否及时修复？ | <input type="checkbox"/> 是 <input type="checkbox"/> 否 |
| 17 | 网站恶意代码防护 | 是否有网页挂马检测系统？ | <input type="checkbox"/> 是 <input type="checkbox"/> 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？ | <input type="checkbox"/> 是 <input type="checkbox"/> 否 |
| | | 关键信息发布是否多级审核？ | <input type="checkbox"/> 是 <input type="checkbox"/> 否 |
| | | 网站发布内容是否过滤？ | <input type="checkbox"/> 是 <input type="checkbox"/> 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）？ | <input type="checkbox"/> 是 <input type="checkbox"/> 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？ | <input type="checkbox"/> 是 <input type="checkbox"/> 否 |
| | | 网站后台管理系统登录是否采取验证机制？ | <input type="checkbox"/> 是 <input type="checkbox"/> 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？ | <input type="checkbox"/> 是 <input type="checkbox"/> 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？ | <input type="checkbox"/> 是 <input type="checkbox"/> 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？ | <input type="checkbox"/> 是 <input type="checkbox"/> 否 |
| | | 网站服务器和数据库服务器是否采用冷备方式？ | <input type="checkbox"/> 是 <input type="checkbox"/> 否 |
| 22 | 网站前、后台系统隔离情况 | 是否采用逻辑隔离？ | <input type="checkbox"/> 是 <input type="checkbox"/> 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？ | <input type="checkbox"/> 是 <input type="checkbox"/> 否 |
| | | 应用远程管理时是否采用加密通道？ | <input type="checkbox"/> 是 <input type="checkbox"/> 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？ | <input type="checkbox"/> 是 <input type="checkbox"/> 否 |
| | | 网站内容远程维护时是否采用加密通道？ | <input type="checkbox"/> 是 <input type="checkbox"/> 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？ | <input type="checkbox"/> 是 <input type="checkbox"/> 否 |
| | | 网站服务器操作系统是否存在弱口令？ | <input type="checkbox"/> 是 <input type="checkbox"/> 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？ | <input type="checkbox"/> 是 <input type="checkbox"/> 否 |
| | | 网站服务器数据库是否共用同一管理口令？ | <input type="checkbox"/> 是 <input type="checkbox"/> 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？ | <input type="checkbox"/> 是 <input type="checkbox"/> 否 |
| | | 网站服务器中间件是否存在弱口令？ | <input type="checkbox"/> 是 <input type="checkbox"/> 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？ | <input type="checkbox"/> 是 <input type="checkbox"/> 否 |
| | | 是否完成网站等级保护备案？ | <input type="checkbox"/> 是 <input type="checkbox"/> 否 |
| | | 是否完成网站统一标识？ | <input type="checkbox"/> 是 <input type="checkbox"/> 否 |