附件一：

电力企业在电力行业网络等级保护中的义务 Q&A:

1. 电力企业应在何时开展网络定级，定级依据是什么？

电力企业应当在**网络规划设计阶段**确定定级对象（网络）及其安全保护等级，并在网络功能、服务范围、服务对象和处理的数据等**发生重大变化时**，及时申请**变更**其安全保护等级。电力企业在定级时依据《网络安全等级保护定级指南》（GB/T 22240）等国家标准规范和电力行业网络安全等级保护定级指南，建议电力企业关注国家能源局制定电力行业网络安全等级保护定级指南的相关动态。

2. 电力企业对网络定级后，还需要开展哪些相关工作？

1) 评审

- 拟定为**第二级及以上**的网络：电力企业应当**组织网络安全专家**进行定级评审。
- 拟定为**第四级及以上**的网络：电力企业除了应当组织网络安全专家进行定级评审外，还应由**国家能源局**统一组织**国家网络安全等级保护专家**进行定级评审。

2) 报审

- 全国电力安全生产委员会企业成员单位汇总集团总部拟定为第二级及以上网络的定级结果和专家评审意见，报**国家能源局**审核。
- 各区域（省）内的电力企业汇总本单位拟定为第二级及以上网络的定级结果，报**国家能源局派出机构**审核。

  国家能源局或其派出机构应在收到审核材料 **30 日**内反馈审核意见。

3) 备案

新建或已运营（运行）的**第二级及以上**网络，应当在收到国家能源局或其派出机构**审核意见后**，向**公安机关**备案并按照第八条规定的定级审核权限向国家能源局或其派出机构报告定级备案结果。

3. 电力企业在报国家能源局或其派出机构审核时，都应提交什么材料？

需要提交如下材料：（1）《电力行业网络安全等级保护定级审核表》；（2）定级审核申请报告；（3）各定级对象的定级报告及相关附件；（4）定级专家评审意见；（5）本企业网络安全管理部门对网络安全等级保护定级的意见。

4. **电力企业如何选择网络产品和服务？**

电力企业应当采购、使用**符合国家法律法规和有关标准规范要求且满足网络安全等级保护需求的网络产品和服务**。特别是对于电力监控系统，应按照《电力监控系统安全防护规定》（国家发展和改革委员会令 2014 年第 14 号）要求，采购和使用电力专用横向单向安全隔离装置、电力专用纵向加密认证装置或者加密认证网关等设备设施；在设备选型及配置时，禁止选用经国家能源局通报存在严重安全漏洞和风险的系统及设备，对已经投入运行的系统及设备应及时整改并加强运行管理和安全防护。需要提醒电力企业注意的是，采购网络产品和服务，影响或可能影响国家安全的，应当依据国家网信部门制定的**网络安全审查办法申报网络安全审查**。

5. 电力企业在网络规划、建设、运营过程中，需要注意什么？

电力企业在网络规划、建设、运营过程中，应当遵循**同步规划、同步建设、同步使用**的原则，按照该网络的安全保护等级要求，建设网络安全设备设施，制定并落实安全管理制度，健全网络安全防护体系。

6. 网络建设完成后，电力企业还需要做哪些网络安全等级保护相关工作？

1) 测评

电力企业应当委托测评机构进行等级保护测评：

- **第二级**网络：每两年应进行一次；
- **第三级及以上**网络：每年一次；
- **新建**的第三级及以上网络：先测评，后运行。

测评机构需组织专家对第三级及以上网络的网络安全等级保护测评报告进行评审。

2) 自查

电力企业应当定期对网络安全状况、安全保护制度及措施的落实情况进行自查。

- **第二级**电力监控系统：每两年至少一次；
- **第三级及以上**网络：每年至少一次。

在测评和自查中，需要注意两点：一是对第三级及以上网络的网络安全等级保护测评报告，相关电力企业应要求测评机构组织专家评审；二是在自查和测评中发现的安全风险隐患，电力企业应制定整改方案，并开展安全建设整改。

3) 报告

电力企业应当按照《等保办法（修订征求意见稿）》第八条规定的定级审核权限，每年向国家能源局或其派出机构报告网络安全等级保护工作情况，包括网络安全等级保护定级备案、等级保护测评、安全建设整改、安全自查等情况。

7. 电力企业在接受国家能源局及派出机构对电力行业网络登记保护的安全监督、检查、指导前，应做那些准备？

电力企业除应按照上述问题的答案中履行相应义务外，还需要准备如下相关的信息资料及数据文件：（1）网络安全等级保护定级备案事项变更情况；（2）网络安全组织、人员、岗位职责的变动情况；（3）网络安全管理制度、措施变更情况；（4）网络运行状况记录；（5）电力企业及上级部门对网络安全状况的检查记录；（6）测评机构出具的网络安全等级保护测评报告；（7）网络安全产品使用的变更情况；（8）网络安全事件应急预案，网络安全事件应急处置结果报告；（9）网络数据容灾备份情况；（10）网络安全建设、整改结果报告；（11）其他需要提供的材料。

对**第三级及以上**网络的电力企业，国家能源局及其派出机构将结合关键信息基础设施网络安全检查，定期组织开展抽查，主要事项有：（1）网络安全等级保护定级工作开展情况，包括定级评审、审核、备案及根据网络安全需求变化调整定级等情况；（2）电力企业网络安全管理制度、措施的落实情况；（3）电力企业及其主管部门对网络安全状况的检查情况；（4）网络安全等级保护测评工作开展情况；（5）网络安全产品使用情况；（6）网络安全建设整改情况；（7）备案材料与电力企业及其网络的符合情况；（8）其他应当进行监督检查的事项。

对**公安机关**开展的网络安全执法检查，电力企业应予以协助、配合。需要特别提醒电力企业注意的是，对在网络安全检查中发现的问题，应当按照网络安全等级保护管理规范和技术标准组织安全建设整改。必要时，还应接受国家能源局及其派出机构对整改情况进行的抽查。

8. 电力企业在选择测评机构时应注意什么？

电力企业在选择测评机构时，应当选择符合条件的测评机构进行网络安全等级保护测评，具体条件如下：

1) 测评机构应获得国家认证认可委员会批准的认证机构发放的《网络安全等级测评与检测评估机构服务认证证书》并纳入《全国网络安全等级测评与检测评估机构目录》；

2) 从事电力监控系统网络安全等级保护测评的机构应熟悉电力监控系统网络安全管理和技术防护要求，具备相应的服务能力和经验。从事电力监控系统第二级网络等级保护测评的机构应具备近 2 年内 30 套以上工业控制系统等级保护测评或风险评估服务经验；从事电力监控系统第三级网络等级保护测评的机构应具备近 3 年内 50 套以上电力监控系统安全防护评估服务经验；从事电力监控系统第四级及以上网络等级保护测评的机构应具备 5 年以上电力监控系统安全防护评估服务经验；

3) 对属于电力行业 CII 的网络，选择测评机构时应保证其安全可信；

4) 禁止选择被国家能源局通报有不良行为或被相关管理部门通报整改的测评机构；

5) 电力企业应采取签署保密协议、开展安全保密培训和现场监督等措施，加强对测评机构、测评人员和测评过程的安全保密管理，避免发生泄密事件或电力安全生产事件。

9. 电力企业在网络安全等级保护中时采用密码的，应当注意什么？

首先，要遵守相关的法律法规和标准。电力企业在采用密码对不涉及国家秘密的网络进行等级保护的，应当遵照《中华人民共和国密码法》等有关法律法规

规定和国家密码管理部门制定的网络安全等级保护密码技术标准执行。电力企业网络安全等级保护中密码的配备、使用和管理等，应当严格执行国家密码管理的有关规定。

其次，要使用符合要求的密码产品和服务。电力企业运用密码技术进行网络安全等级保护建设与整改时，应采用商用密码检测、认证机构检测认证合格的商用密码产品和服务。涉及商用密码进口的，还应当符合国家商用密码进口许可有关要求。

再次，对第三级及以上网络，电力企业应特别注意。应在网络规划、建设和运行阶段，按照商用密码应用安全性评估管理办法和标准规范，自行或者委托商用密码检测机构开展商用密码应用安全性评估工作。

最后，配合检查，及时整改。电力企业应当积极配合各级密码管理部门对网络安全等级保护工作中密码配备、使用和管理的情况进行检查和安全性评估。对于检查和安全性评估发现的问题，应当按照国家密码管理的相关规定要求及时整改。

附件二：

电力企业的一般职责	
职责	具体内容
网络安全主体责任	电力企业**主要负责人**是本单位网络安全的第一责任人。电力企业应当建立健全网络安全管理、评价考核制度体系，应当成立**工作领导机构**，明确责任部门，设立专职岗位，定义岗位职责，明确人员分工和技能要求，建立健全网络安全责任制。
网络安全保护与监测	➢ 电力企业应当按照电力监控系统安全防护规定、关键信息基础设施安全保护制度、数据安全保护制度及网络安全审查工作机制的要求，对本单位的**网络与信息系统进行安全保护**，并将网络安全纳入安全生产管理体系； ➢ 电力企业应当按照国家**网络安全等级保护**制度，对本单位的网络与信息系统进行安全保护，并将网络安全纳入安全生产管理体系[1]。 ➢ 电力企业应当依据国家和行业相关标准、规程和规范开展**网络安全技术监督工作**，可委托网络安全服务机构协助开展； ➢ 电力企业应当建立健全本单位网络安全监测预警和信息通报机制，及时掌握本单位网络安全运行状况、安全态势，**及时处置网络安全威胁与隐患**，定期向国家能源局和地方能源主管部门报告有关情况。
信息系统建设	➢ 电力企业规划设计信息系统时，应当明确系统的安全保护需求，保证安全技术措施**同步规划、同步建设、同步使用**，设计合理的总体安全方案并经专业技术人员评审通过，制定安全实施计划，负责信息系统安全建设工程的实施。信息系统上线前，电力企业应委托网络安全服务机构开展第三方安全测试。
网络安全产品采购	➢ 电力企业应当选用符合国家有关规定、满足网络安全要求的信息技术产品和服务，开展信息系统安全建设或改建工作。 ➢ **接入生产控制大区的涉网安全产品需经电力调度机构同意**； ➢ 电力企业**禁止选择**被国家能源局通报有不良行为或被相关管理部门通报整改的网络安全服务机构； ➢ 电力企业应当建立健全网络产品安全漏洞信息接收渠道并保持畅通，发现存在安全漏洞后，应当立即采取措施，及时对安全漏洞进行验证与修补； ➢ 电力企业应当督促电力监控系统专用安全产品研发单位和供应商按国家有关要求做好保密工作，防止关键技术泄露。**严禁在互联网上销售、购买电力监控系统专用安全产品。**

[1] 电力企业在电力行业网络等级保护中的具体义务请见附件。

评估与检测	➢ 电力企业应当按照国家有关规定开展**电力监控系统安全防护评估、网络安全等级保护测评、关键信息基础设施安全检测和风险评估、商用密码应用安全性评估和网络安全审查**等工作，未达到要求的应当及时进行整改； ➢ 电力企业应当按照国家有关规定开展**网络安全风险评估**工作，建立健全网络安全风险评估的自评估和检查评估制度，完善网络安全风险管理机制。发现风险隐患可能对电力行业网络安全产生较大影响的，应当向国家能源局和地方能源主管部门报告；
应急处置	➢ 电力企业应当按照电力行业网络安全事件**应急预案，**制修订本单位网络安全事件应急预案，**每年至少开展一次应急演练**。制修订电力监控系统专项网络安全事件应急预案并定期组织演练。定期组织开展网络攻防演习，检验安全防护和应急处置能力。 ➢ 电力企业应当在国家**重要活动、会议期间**结合实际制定网络安全保障专项工作方案和应急预案，成立保障组织机构，明确目标任务，细化措施要求，组织预案演练，确保重要信息系统、电力监控系统安全稳定运行。 ➢ 电力企业发生网络安全事件后，应当**立即启动网络安全事件应急预案，**及时采取有效措施，消除安全隐患，防止危害扩大，尽可能保护好现场，按规定做好信息**上报**工作。
数据安全和个人信息保护	➢ 电力企业应当建立健全**全流程数据安全管理和个人信息保护制度**，按照国家和行业**重要数据目录及数据分类分级保护**相关要求，确定本单位的重要数据具体目录，对列入目录的数据进行重点保护。
容灾备份	➢ 电力企业应当按照国家有关规定，建立健全**容灾备份**制度，对关键系统和重要数据进行有效备份。
资金保障	➢ 电力企业应当建立网络安全资金保障制度，**安排网络安全专项预算，确保网络安全投入不低于信息化总投入的 5%。**
员工培训和人员意识教育	➢ 电力企业应当加强网络安全从业人员**考核和管理**，做好全员**网络安全宣传教育，提高网络安全意识**。从业人员应当定期接受相应的政策规范和专业技能培训，并经培训合格后上岗。
报送	➢ 电力企业应依法依规开展**关键信息基础设施**认定、报送工作，关键信息基础设施发生重大变化，可能影响其认定结果的，应及时将相关情况报告国家能源局和地方能源主管部门。 ➢ 电力企业应当于每**年 11 月 1 日**前，将当年网络安全工作的专项总结报送国家能源局及其派出机构、地方能源主管部门。