商用密码应用安全性评估管理办法

（国家密码管理局令第3号）

第一条　为了规范商用密码应用安全性评估工作，保障网络与信息安全，维护国家安全和社会公共利益，保护公民、法人和其他组织的合法权益，根据《中华人民共和国密码法》、《商用密码管理条例》等有关法律法规，制定本办法。

第二条　本办法所称商用密码应用安全性评估，是指按照有关法律法规和标准规范，对网络与信息系统使用商用密码技术、产品和服务的合规性、正确性、有效性进行检测分析和评估验证的活动。

第三条　国家密码管理局负责管理全国的商用密码应用安全性评估工作。县级以上地方各级密码管理部门负责管理本行政区域的商用密码应用安全性评估工作。

国家机关和涉及商用密码工作的单位在其职责范围内负责指导、监督本机关、本单位或者本系统的商用密码应用安全性评估工作。

第四条　从事商用密码应用安全性评估活动，向社会出具具有证明作用的商用密码应用安全性评估数据、结果的机构，应当经国家密码管理局认定，依法取得商用密码检测机构资质。

第五条　国家密码管理局支持商用密码应用安全性评估技术、标准、工具创新，完善商用密码应用安全性评估标准体系，鼓励设立商用密码应用安全性评估行业组织，加强行业自律，维护行业秩序。

第六条　法律、行政法规和国家有关规定要求使用商用密码进行保护的网络与信息系统（以下简称重要网络与信息系统），其运营者应当使用商用密码进行保护，制定商用密码应用方案，配备必要的资金和专业人员，同步规划、同步建设、同步运行商用密码保障系统，并定期开展商用密码应用安全性评估。

第七条　重要网络与信息系统规划阶段，其运营者应当依照相关法律法规和标准规范，根据商用密码应用需求，制定商用密码应用方案，规划商用密码保障系统。

重要网络与信息系统的运营者应当自行或者委托商用密码检测机构对商用密码应用方案进行商用密码应用安全性评估。商用密码应用方案未通过商用密码应用安全性评估的，不得作为商用密码保障系统的建设依据。

第八条　重要网络与信息系统建设阶段，其运营者应当按照通过商用密码应用安全性评估的商用密码应用方案组织实施，落实商用密码安全防护措施，建设商用密码保障系统。

重要网络与信息系统运行前，其运营者应当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。网络与信息系统未通过商用密码应用安全性评估的，运营者应当进行改造，改造期间不得投入运行。

第九条　重要网络与信息系统建成运行后，其运营者应当自行或者委托商用密码检测机构每年至少开展一次商用密码应用安全性评估，确保商用密码保障系统正确有效运行。

未通过商用密码应用安全性评估的，运营者应当进行改造，并在改造期间采取必要措施保证网络与信息系统运行安全。

第十条　对商用密码应用方案开展商用密码应用安全性评估，应当包括以下内容:

（一）考量商用密码应用需求的全面性、合理性和针对性，对照相关标准规范选取适用指标的准确性，以及不适用指标论证的充分性;

（二）分析商用密码应用流程和机制是否具备可实施性、商用密码保护措施是否达到相应的商用密码应用要求、相关描述是否详尽;

（三）论证商用密码技术、产品和服务选用的合规性，密钥管理的安全性，以及使用商用密码解决安全风险的科学性;

（四）编制形成商用密码应用安全性评估报告。

第十一条　对建设完成的网络与信息系统开展商用密码应用安全性评估，应当包括以下内容:

（一）对照商用密码应用方案，了解网络与信息系统基本情况，准确划定评估范围;

（二）确定评估指标及评估对象，论证编制商用密码应用安全性评估实施方案;

（三）依据商用密码应用安全性评估实施方案，开展现场评估，做好数据采集和信息汇总，研判商用密码保障系统配置及运行情况;

（四）根据客观凭据逐项对评估指标进行判定，编制形成商用密码应用安全性评估报告。

第十二条　运营者开展商用密码应用安全性评估活动，应当遵守法律法规、标准规范要求，遵循客观实际、科学公正、诚实信用原则。委托商用密码检测机构开展商用密码应用安全性评估的，不得对评估结果施加不当影响，并应当提供以下支持:

（一）对网络与信息系统的重要数据进行备份;

（二）提供完整有效的网络与信息系统设备清单和网络拓扑;

（三）提供详细的网络与信息系统商用密码应用方案、密码相关管理制度和密码配置、运行、维护记录;

（四）提供商用密码产品管理入口、网络交换设备接入端口等相关信息、数据接入分析条件，并配合进行数据采集;

（五）安排网络与信息系统相关网络管理员、系统管理员、密钥管理员、密码安全审计员、密码操作员等做好配合;

（六）其他需要配合的事项。

第十三条　自行开展商用密码应用安全性评估的网络与信息系统，其运营者应当符合以下要求:

（一）具有与开展商用密码应用安全性评估活动相适应的设备设施;

（二）具有与开展商用密码应用安全性评估活动相适应的项目管理、质量管理、人员管理、档案管理、安全保密管理等规章制度;

（三）具有与开展商用密码应用安全性评估活动相适应的专业人员；

（四）具有与开展商用密码应用安全性评估活动相适应的专业能力。

自行开展商用密码应用安全性评估形成的商用密码应用安全性评估报告，应当符合相关国家标准、行业标准和有关规定的要求，由本单位密码或者网络安全负责人签字确认并加盖本单位公章。

运营者应当对商用密码应用安全性评估原始记录和商用密码应用安全性评估报告归档留存，保证其具有可追溯性。商用密码应用安全性评估原始记录和商用密码应用安全性评估报告的保存期限不得少于6年。

第十四条　重要网络与信息系统的运营者应当在商用密码应用安全性评估报告形成后30日内，将评估报告和相关工作情况按照国家有关规定报送国家密码管理局或者网络与信息系统所在地省、自治区、直辖市密码管理部门备案。

国家密码管理局或者省、自治区、直辖市密码管理部门对商用密码应用安全性评估结果备案材料进行形式审查。形式审查未通过的，相关运营者应当重新提交备案材料。

国家密码管理局可以对商用密码应用安全性评估结果进行抽样检查。抽样检查不合格的，相关运营者应当重新开展商用密码应用安全性评估。

省、自治区、直辖市密码管理部门应当按季度向国家密码管理局报送本地区商用密码应用安全性评估工作开展情况。

第十五条　运营者发现密码相关重大安全事件、重大密码安全隐患或者特殊紧急情况的，应当及时向国家密码管理局或者网络与信息系统所在地省、自治区、直辖市密码管理部门报告，并启动应急处置方案，必要时开展商用密码应用安全性评估。

第十六条　县级以上地方各级密码管理部门、国家机关和涉及商用密码工作的单位可以根据工作需要，对本地区、本机关、本单位或者本系统的重要网络与信息系统商用密码应用安全性评估情况开展专项检查。

第十七条　重要网络与信息系统的运营者违反《中华人民共和国密码法》、《商用密码管理条例》和本办法规定，有下列情形之一的，由密码管理部门责令改正，给予警告；拒不改正或者有其他严重情节的，处10万元以上100万元以下罚款，对直接负责的主管人员处1万元以上10万元以下罚款：

（一）重要网络与信息系统规划阶段，未对商用密码应用方案进行商用密码应用安全性评估的；

（二）重要网络与信息系统建设阶段，未按照通过商用密码应用安全性评估的商用密码应用方案建设商用密码保障系统的；

（三）重要网络与信息系统运行前，未开展商用密码应用安全性评估的；

（四）重要网络与信息系统运行前，未通过商用密码应用安全性评估且未进行改造的；

（五）重要网络与信息系统建成运行后，未定期开展商用密码应用安全性评估的；

（六）重要网络与信息系统建成运行后，未通过定期开展的商用密码应用安全性评估且未进行改造的；

（七）违反法律法规、标准规范要求开展商用密码应用安全性评估的；

（八）不符合相关要求自行开展商用密码应用安全性评估的。

第十八条　重要网络与信息系统的运营者违反本办法规定，有下列情形之一的，由密码管理部门责令改正；逾期未改正或者改正后仍不符合要求的，处1万元以上10万元以下罚款，对直接负责的主管人员处5000元以上5万元以下罚款：

（一）对商用密码应用安全性评估结果施加不当影响的；

（二）未为商用密码应用安全性评估活动提供必要支持的；

（三）未按照要求进行商用密码应用安全性评估结果备案的。

第十九条　从事商用密码应用安全性评估监督管理工作的人员滥用职权、玩忽职守、徇私舞弊，或者泄露、非法

向他人提供在履行职责中知悉的商业秘密、个人隐私、举报人信息的，依法给予处分。

第二十条　本办法施行前正在建设的重要网络与信息系统，其运营者应当加强商用密码应用方案编制论证，建设完善商用密码保障系统，并按照本办法第八条规定开展商用密码应用安全性评估。

本办法施行前已经投入运行的重要网络与信息系统，其运营者应当按照本办法第九条规定开展商用密码应用安全性评估。

第二十一条　本办法自 2023 年 11 月 1 日起施行。