关键信息基础设施商用密码使用管理规定

2025年07月01日 20:30 来源： 中国网信网

国家密码管理局

国家互联网信息办公室

中华人民共和国公安部

令

第5号

《关键信息基础设施商用密码使用管理规定》已经2025年4月21日国家密码管理局局务会议审议通过，并经国家互联网信息办公室、公安部同意，现予公布，自2025年8月1日起施行。

国家密码管理局局长 刘东方

国家互联网信息办公室主任 庄荣文

公安部部长 王小洪

2025年6月11日

关键信息基础设施商用密码使用管理规定

第一条 为规范关键信息基础设施商用密码使用，保护关键信息基础设施安全，根据《中华人民共和国密码法》、《中华人民共和国网络安全法》、《中华人民共和国数据安全法》、《中华人民共和国个人信息保护法》、《商用密码管理条例》和《关键信息基础设施安全保护条例》、《网络数据安全管理条例》等有关法律、行政法规，制定本规定。

第二条 依据《中华人民共和国网络安全法》、《关键信息基础设施安全保护条例》等法律、行政法规和国家有关规定认定的关键信息基础设施的商用密码使用管理，适用本规定。

第三条 国家密码管理部门会同国家网信部门、国务院公安部门负责规划、指导和监督全国的关键信息基础设施商用密码使用管理工作，建立关键信息基础设施商用密码使用管理信息共享机制。

县级以上地方各级密码管理部门会同网信部门、公安机关负责指导和监督本行政区域的关键信息基础设施商用密码使用管理工作。

第四条 关键信息基础设施保护工作部门（以下简称保护工作部门）在职责范围内负责监督管理本行业、本领域关键信息基础设施商用密码使用工作，单独编制本行业、本领域商用密码使用规划或者纳入本行业、本领域的关键信息基础设施安全规划并组织实施，指导本行业、本领域关键信息基础设施运营者（以下简称运营者）开展商用密码相关制度、人员、经费等保障工作。

保护工作部门应当于每年3月31日前向国家密码管理部门、国家网信部门、国务院公安部门报告上一年度本行业、本领域关键信息基础设施商用密码使用管理情况。

关键信息基础设施发生涉及商用密码的重大网络安全事件或者发现涉及商用密码的重大网络安全威胁时，保护工作部门应当及时向国家密码管理部门、国家网信部门、国务院公安部门报告，指导运营者开展应急处置，必要时开展商用密码应用安全性评估。

第五条 运营者应当按照相关法律、行政法规和国家有关规定，遵循国家商用密码管理、网络安全等级保护、关键信息基础设施安全保护等制度要求，使用商用密码保护关键信息基础设施，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。

运营者应当于每年1月31日前向所属的保护工作部门报告上一年度关键信息基础设施商用密码使用以及商用密码应用安全性评估开展情况。

第六条 运营者应当加强关键信息基础设施商用密码使用制度保障，建立商用密码使用、应急处置、重大事件报告等关键信息基础设施商用密码使用管理制度。

运营者的主要负责人对关键信息基础设施商用密码使用管理负总责，负责关键信息基础设施商用密码使用和涉及商用密码的重大网络安全事件处置工作。

第七条 运营者应当加强关键信息基础设施商用密码使用人员保障，配备取得密码相关专业学历或者密码相关国家职业技能等级认定证书的专业人员分别承担密钥管理员、密码操作员等职责，配备具有安全审计专业能力的人员承担密码安全审计员职责。

运营者应当对密码相关专业人员进行安全背景审查，并定期组织其参加密码相关业务技能培训，提高密码相关专业人员的商用密码使用能力。

第八条 运营者应当加强关键信息基础设施商用密码使用和应用安全性评估经费保障，将商用密码使用和应用安全性评估经费纳入网络安全和信息化经费安排。

第九条 关键信息基础设施使用的商用密码产品、服务应当经检测认证合格，使用的密码算法、密码协议、密钥管理机制等商用密码技术应当通过国家密码管理部门审查鉴定。

运营者采购涉及商用密码的网络产品和服务，影响或者可能影响国家安全的，应当按照《网络安全审查办法》进行网络安全审查。

第十条 关键信息基础设施应当按照国家数据安全保护、个人信息保护有关要求，使用商用密码对其存储、使用、传输的核心数据、重要数据和个人信息进行保护。

第十一条 关键信息基础设施规划阶段，其运营者应当依照相关法律、行政法规和标准规范，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并纳入关键信息基础设施安全规划统筹部署。

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。

第十二条 关键信息基础设施建设阶段，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。建设过程中需要调整商用密码应用方案的，应当重新开展商用密码应用安全性评估，评估通过后方可按照调整后的商用密码应用方案继续建设。

关键信息基础设施运行前，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。关键信息基础设施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。

第十三条 关键信息基础设施建成运行后，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，确保关键信息基础设施商用密码的正确使用和商用密码保障系统的有效运行。关键信息基础设施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关键信息基础设施运行安全。

第十四条 本规定施行前正在建设的关键信息基础设施，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，并按照本规定第十二条开展商用密码应用安全性评估。

本规定施行前已经投入运行的关键信息基础设施，其运营者应当按照本规定第十三条开展商用密码应用安全性评估。

第十五条 开展关键信息基础设施商用密码应用安全性评估，应当符合《商用密码应用安全性评估管理办法》有关规定。

关键信息基础设施商用密码应用安全性评估应当与关键信息基础设施安全检测评估、网络安全等级测评加强衔接，避免重复评估、测评。

第十六条 国家密码管理部门负责建设和管理国家关键信息基础设施商用密码运行安全管理基础设施，统筹保护工作部门建设本行业、本领域关键信息基础设施商用密码运行安全管理基础设施，会同国家网信部门、国务院公安部门分析研判关键信息基础设施商用密码运行安全态势，协同应对处置重大商用密码运行安全威胁。

第十七条 密码管理部门应当定期组织开展关键信息基础设施商用密码使用情况监督检查。保护工作部门应当定期对本行业、本领域关键信息基础设施商用密码使用情况进行检查并提出改进措施，必要时可以自行或者委托商用密码检测机构等专业机构进行商用密码应用安全性评估。

运营者对密码管理部门和保护工作部门开展的关键信息基础设施商用密码使用情况监督检查应当予以配合，根据监督检查意见及时进行整改并向保护工作部门报告整改情况，保护工作部门应当将整改情况向国家密码管理部门报告。

开展关键信息基础设施商用密码使用情况监督检查应当加强协同配合、信息沟通，避免不必要的检查和交叉重复检查。监督检查不得收取费用，不得要求被监督检查单位购买、使用指定单位或者指定品牌的商用密码产品、服务。

第十八条 密码管理部门、有关部门、商用密码检测机构及其工作人员对其在履行职责中知悉的国家秘密、商业秘密和个人隐私承担保密义务，不得泄露或者非法向他人提供。

第十九条 运营者违反《中华人民共和国密码法》、《中华人民共和国网络安全法》、《商用密码管理条例》、《关键信息基础设施安全保护条例》和本规定有关条款，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）未按照要求使用商用密码保护关键信息基础设施，同步规划、同步建设、同步运行商用密码保障系统的；

（二）关键信息基础设施使用的商用密码产品、服务未经检测认证合格的；

（三）关键信息基础设施使用的密码算法、密码协议、密钥管理机制等商用密码技术未通过国家密码管理部门审查鉴定的；

（四）关键信息基础设施规划阶段，未制定商用密码应用方案，或者未对商用密码应用方案进行商用密码应用安全性评估的；

（五）关键信息基础设施建设阶段，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；

（六）关键信息基础设施运行前，未开展商用密码应用安全性评估，或者未通过商用密码应用安全性评估且未进行改造的；

（七）关键信息基础设施建成运行后，未定期开展商用密码应用安全性评估，或者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。

第二十条 运营者违反《中华人民共和国密码法》、《中华人民共和国网络安全法》、《商用密码管理条例》、《关键信息基础设施安全保护条例》和本规定第九条，使用未经安全审查或者安全审查未通过的涉及商用密码的网络产品或者服务的，由有关主管部门责令停止使用，处采购金额1倍以上10倍以下罚款；对直接负责的主管人员和其他直接责任人员处1万元以上10万元以下罚款。

第二十一条 运营者违反《中华人民共和国密码法》、《中华人民共和国网络安全法》、《商用密码管理条例》、《关键信息基础设施安全保护条例》和本规定第十七条，无正当理由拒不接受、不配合或者干预、阻挠密码管理部门、有关部门的商用密码监督管理的，由密码管理部门、有关部门责令改正，给予警告；拒不改正或者有其他严重情节的，处5万元以上50万元以下罚款，对直接负责的主管人员和其他直接责任人员处1万元以上10万元以下罚款；情节特别严重的，责令停业整顿。

第二十二条 运营者违反本规定，有下列情形之一的，由密码管理部门、有关部门依据职责责令改正：

（一）未按照要求报告上一年度关键信息基础设施商用密码使用以及商用密码应用安全性评估开展情况的；

（二）未建立关键信息基础设施商用密码使用管理制度的；

（三）未按照要求配备密钥管理员、密码操作员、密码安全审计员的；

（四）未保障关键信息基础设施商用密码使用和应用安全性评估经费的。

第二十三条 从事关键信息基础设施商用密码使用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。

第二十四条 属于国家政务信息系统的关键信息基础设施的商用密码使用管理，除应当遵守本规定以外，还应当按照《国家政务信息化项目建设管理办法》（国办发〔2019〕57号）等有关规定要求执行。

第二十五条 本规定自2025年8月1日起施行。