



中国密码学会
密评联委会

2023

商用密码应用安全性评估 发展研究报告

中国密码学会商用密码应用安全性评估联合委员会

2023年8月

前言

当前，世界之变、时代之变、历史之变正以前所未有的方式展开，党的二十大报告为我们擘画了以中国式现代化推进中华民族伟大复兴的宏伟蓝图，开启了全面建成社会主义现代化强国、实现第二个百年奋斗目标的新征程。这举旗定向的政治宣言、引领复兴的行动纲领以专章论述“推进国家安全体系和能力现代化，坚决维护国家安全和社会稳定”，指出“必须坚定不移贯彻总体国家安全观，把维护国家安全贯穿党和国家工作各方面全过程，确保国家安全和社会稳定。”

网络安全是国家安全的重要组成部分，密码作为国之重器，是保障网络与数据安全的核心技术，是数字经济高质量发展的基础，是推进中国式现代化的重要支撑。商用密码应用安全性评估（以下简称密评），作为密码应用管理过程的重要组成部分和不可缺失的环节，是发挥密码作用的重要抓手。密评活动贯穿于密码应用管理整个生命周期，对维护网络和数据安全、赋能数字经济、护航中国式现代化发展具有重要意义。

我国高度重视密评工作，出台多项顶层战略规划和法律法规，要求在重点领域和关键环节开展密评，为密评工作提供了合规驱动力。各地区、各领域积极落实密评要求，加强密评政策引导，加速推动密码在金融、通信、公安、税务、社保、交通、卫生健康、能源、电子政务等领域中的应用。在国家密码管理局的指导下，密评工作机制不断健全，密评机构能力进一步增强，密评活动标准化工作持续推进，密评程序逐步完善，密评进入蓬勃发展时期。未来，密评将焕发出更强的生命力和活力，持续为保障数字经济安全、助力现代化强国建设发挥积极作用。

2023年7月1日，《商用密码管理条例》正式施行，标志着密评从试点建设迈向依法管理的新阶段。站在推进密评法制化建设的新起点，本报告总结了密评相关政策法规要求及密评体系建设进展，分析了密评行业发展情况，并对密评工作未来发展提出了建议，为密评相关工作者提供参考。



版权声明

本报告版权属于中国密码学会商用密码应用安全性评估联合委员会，并受法律保护。转载、摘编或以其他方式使用报告文字或观点的，均应注明“来源：中国密码学会商用密码应用安全性评估联合委员会”或“来源：密评联委会”。违反以上声明者，中国密码学会商用密码应用安全性评估联合委员会将保留追究其相关法律责任的权利。

本报告主要编写单位：中国工业互联网研究院（工业和信息化部密码应用研究中心）、深圳市网安计算机安全检测技术有限公司、北京炼石网络技术有限公司、江苏省信息安全测评中心、中国电子科技集团公司第十五研究所、工业和信息化部电子第五研究所、中国电子信息产业发展研究院、中国信息通信研究院

本报告主要编写人员：王聪、唐明环、查奇文、王伟忠、彭浩楠、杨宏志、孙少波、白小勇、钱晶、魏婷、张齐军、张腾标、衡帅、刘健、杨龙、韦永霜、张皓涵、王东阳、李佳曦



目 录

引言	1
1/ 密评相关政策法规要求	2
1.1 国家法律法规布局密评顶层设计	2
1.2 国家多项政策文件为密评实施提供指引	3
1.3 有关部门出台指导性 & 规范性文件落实密评要求	4
1.4 相关地区积极将密评要求纳入地方政策制度	5
2/ 密评体系建设进展	5
2.1 密评工作机制	6
2.2 密评机构培育	8
2.3 密评系列标准	9
2.4 密评程序	13
3/ 密评行业发展情况	15
3.1 密评试点机构规模布局日趋合理	15
3.2 密评人才供给能力持续提升	17
3.3 密评覆盖范围逐年扩大	17
4/ 发展建议	21
附录 1：密评相关法规政策汇总	22
1.1 国家层面密码应用及密评相关法律法规	22
1.2 国家层面密码应用及密评相关政策文件	24
1.3 各部门密码应用及密评相关政策文件	25
1.4 各省（自治区、直辖市）及新疆生产建设兵团密码应用及密评相关政策文件	29
附录 2：密评相关标准与指导性文件列表	48
附录 3：密评大事记	49

引言

在数字经济时代，密码作为国家重要战略资源，广泛应用于国民经济发展和社会生产生活的方方面面，涵盖金融和通信、公安、税务、社保、交通、卫生健康、能源、电子政务等重要领域，是保障网络与信息安全的核心技术和基础支撑。在推动数字经济高质量发展、推进中国式现代的进程中，如何更好地规范商用密码应用和管理、发挥密码在保障网络安全中的核心支撑作用至关重要。商用密码应用安全性评估作为验证密码应用科学性的有效手段和方法，既是应对网络安全严峻形势的迫切需要，也是落实国家重要领域和关键行业网络安全防护责任的有效手段，更是全面贯彻落实《中华人民共和国密码法》（以下简称《密码法》）和《商用密码管理条例》基本要求、推进商用密码法治建设的重要举措。

密码应用涉及密码算法、技术、产品、服务、密钥管理等多个方面。在当前密码应用实践中，由于密码专业技术人员保障不足，密码应用要求理解把握不到位，密码错用、误用情况经常发生。商用密码应用安全性评估依据科学全面的测评标准，由专业的技术人员采用专业的技术手段和测评工具，科学直观地对信息系统密码应用情况给出评价，发现信息系统密码应用存在的不规范、不安全、不正确等问题，给出专业、可行的意见建议，为网络运营者掌握系统密码应用情况并进一步开展密码应用改造提供支撑，有效规范密码应用，提升网络安全保障水平。



1

密评相关政策法规要求

商用密码应用安全性评估（以下简称密评）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¹。密评是衡量与改进网络与信息系统密码保障水平的关键技术措施，对密码应用的助力推动和网络安全的兜底保障作用突出。我国立足国情将密评相关工作要求纳入顶层设计，出台法律法规、政策文件，推动密评体系不断完善，密评工作进入新发展阶段。

1.1 国家法律法规布局密评顶层设计

我国充分适应新时代商用密码事业发展需要，坚持密评的立法、司法、执法和守法协同推进，通过法律法规明确密评的重要定位、评估范围、责任主体和评估要求等深刻内涵，推动密评在重要领域和关键环节加速推广普及，为数字经济高质量发展提供基础支撑。

表 1 密评相关法律法规要求

法律法规	主要要求
《密码法》	第二十七条 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关键信息基础设施，其运营者应当使用商用密码进行保护，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。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、网络安全等级测评制度相衔接，避免重复评估、测评。
《商用密码管理条例》（2023 年 7 月 1 日施行）	第三十八条 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关键信息基础设施，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，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。 前款所列关键信息基础设施通过商用密码应用安全性评估方可投入运行，运行后每年至少进行一次评估，评估情况按照国家有关规定报送国家密码管理部门或者关键信息基础设施所在地省、自治区、直辖市密码管理部门备案。 第四十一条 网络运营者应当按照国家网络安全等级保护制度要求，使用商用密码保护网络安全。国家密码管理部门根据网络的安全保护等级，确定商用密码的使用、管理和应用安全性评估要求，制定网络安全等级保护密码标准规范。 第四十二条 商用密码应用安全性评估、关键信息基础设施安全检测评估、网络安全等级测评应当加强衔接，避免重复评估、测评。

¹ 《商用密码应用安全性评估管理办法（征求意见稿）》，http://sca.gov.cn/sca/hdjl/2023-06/09/content_1061072.shtml

法律法规	主要要求
《关键信息基础设施安全保护条例》	第五十条 关键信息基础设施中的密码使用和管理，还应当遵守相关法律、行政法规的规定。
《网络安全等级保护条例（征求意见稿）》	第四十七条 非涉密网络应当按照国家密码管理法律法规和标准的要求，使用密码技术、产品和服务。第三级以上网络应当采用密码保护，并使用国家密码管理部门认可的密码技术、产品和服务。 第三级以上网络运营者应在网络规划、建设和运行阶段，按照密码应用安全性评估管理办法和相关标准，委托密码应用安全性测评机构开展密码应用安全性评估。网络通过评估后，方可上线运行，并在投入运行后，每年至少组织一次评估。密码应用安全性评估结果应当报受理备案的公安机关和所在地设区市的密码管理部门备案。

《密码法》明确关键信息基础设施运营者作为第一责任人，应使用商用密码对关键信息基础设施进行保护，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。

《商用密码管理条例》进一步细化了关键信息基础设施商用密码应用与安全性评估要求，明确关键信息基础设施应在规划、建设等必要阶段进行评估，投入运行后，还应当定期开展评估。同时，《商用密码管理条例》明确，网络运营者应当按照国家网络安全等级保护制度要求，使用商用密码保护网络安全。网络安全等级保护制度中的商用密码使用、管理和应用安全性评估要求重点适用对象是第三级以上网络，凸显了对网络安全等级保护三级以上网络加强商用密码应用安全性评估工作、落实商用密码应用相关要求的迫切需要。

《关键信息基础设施安全保护条例》明确，关键信息基础设施中的密码使用和管理，还应当遵守相关法律、行政法规的规定。这对使用密码技术保护关键信息基础设施安全提出了原则性要求。

《网络安全等级保护条例（征求意见稿）》第五章中明确提出密码配备使用、管理和应用安全性评估的有关要求，对网络的密码保护作出规定。其中，对非涉密网络、第三级以上网络提出密码保护要求，明确规定网络运营者应在网络规划、建设和运行阶段委托专业测评机构开展密码应用安全性评估，并对评估结果备案提出了要求²。

1.2 国家多项政策文件为密评实施提供指引

面对新时代全球安全形势及发展需求，我国统筹发展与安全，出台了多项政策文件对密评进行整体性制度安排，推动密评体系健全完善。密评相关国家政策文件要求如表 2 所示，更多国家层面密码应用及密评相关政策文件详见附录 1.2。

2 《网络安全等级保护条例（征求意见稿）》解读，<https://www.secrss.com/articles/5005>



表 2 密评相关国家政策文件要求

文件名称	密评相关工作要求
密码应用与创新发展相关工作规划	全面提升密码基础支撑能力，完善密码应用安全性评估审查机制。
《“十四五”数字经济发展规划》	加强网络安全等级保护和密码应用安全性评估。
《国家政务信息化项目建设管理办法》（国办发〔2019〕57号）	项目建设单位应当落实国家密码管理有关法律法规和标准规范的要求，同步规划、同步建设、同步运行密码保障系统并定期进行评估。
《国务院关于加强数字政府建设的指导意见》（国发〔2022〕14号）	建立健全网络安全、保密监测预警和密码应用安全性评估的机制。

1.3 有关部门出台指导性及规范性文件落实密评要求

据不完全统计，国家密码管理局、中央网信办、教育部、工业和信息化部、公安部、财政部、交通运输部、国家能源局、国家邮政局等部门出台多项密评政策文件，明确金融、政务、教育、工信、交通、能源等行业商用密码应用安全性评估工作要求，提升商用密码应用和管理水平，深化商用密码在各行业或领域的应用。密评相关行业政策文件要求如表 3 所示，更多各部门密码应用及密评相关政策文件详见附录 1.3。

表 3 密评相关行业政策文件要求

有关部门	文件名称	密评相关内容
国家密码管理局、中央网信办、国家发展改革委、科技部、工业和信息化部、公安部、财政部、国务院国资委、市场监管总局、证监会	促进商用密码产业高质量发展相关文件	依法督促建设密码保障体系，并强化重要网络与信息系统商用密码应用安全性评估的执法检查。
教育部	《2020 年教育信息化和网络安全工作要点》（教科技厅〔2020〕1 号）	有序推动教育重要业务信息系统开展密码应用安全性评估，推动国家教育管理信息系统密码普遍应用，提升系统安全和数据安全。
工业和信息化部	《关于加强车联网网络安全和数据安全工作的通知》（工信部网安〔2021〕134 号）	认定为关键信息基础设施的，要按照国家有关标准使用商用密码进行保护，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。
公安部	《贯彻落实网络安全等级保护制度和关键信息基础设施安全保护制度的指导意见》（公网安〔2020〕1960 号）	第三级以上网络运营者应在网络规划、建设和运行阶段，按照密码应用安全性评估管理办法和相关标准，在网络安全等级测评中同步开展密码应用安全性评估。
财政部	《政务信息系统政府采购管理暂行办法》（财库〔2017〕210 号）	采购需求应当落实国家密码管理有关法律法规、政策和标准规范的要求，同步规划、同步建设、同步运行密码保障系统并定期进行评估。

有关部门	文件名称	密评相关内容
交通运输部	《公路水路关键信息基础设施安全保护管理办法》	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公路水路关键信息基础设施，其运营者应当使用商用密码进行保护，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。 商用密码应用安全性评估应当与公路水路关键信息基础设施安全检测评估、网络安全等级测评制度相衔接，避免重复评估、测评。
国家能源局	《关于印发〈电力行业网络安全管理办法〉的通知》（国能发安全规〔2022〕100号）	电力企业应当按照国家有关规定开展商用密码应用安全性评估等工作，未达到要求的应当及时进行整改。
国家邮政局、国家发展改革委、交通运输部	《“十四五”邮政业发展规划》	在网络建设和运营过程中，同步规划、建设、使用有关安全保护措施，严格落实国家关于等保、关保、密评等有关要求。

1.4 相关地区积极将密评要求纳入地方政策制度

据不完全统计，我国各省（自治区、直辖市）及新疆生产建设兵团共出台 130 余项密码应用及密评相关政策文件，针对性提出适应地方特点的信息系统商用密码应用工作要求，推进商用密码应用及安全性评估工作，切实提升信息系统的安全性和密码应用合规性。各省（自治区、直辖市）及新疆生产建设兵团密码应用及密评相关政策详见附录 1.4。

2

密评体系建设进展

2017 年 4 月，国家密码管理局印发《关于开展密码应用安全性评估试点工作的通知》（国密局字〔2017〕138 号），附《商用密码应用安全性评估管理办法（试行）》，开始开展商用密码应用安全性评估试点及机构培育工作。2017 年 9 月，国家密码管理局印发《商用密码应用安全性测评机构管理办法（试行）》等文件，密评制度体系初步建立。2019 年 4 月，为支撑密评各项工作开展，中国密码学会设立商用密码应用安全性评估联合委员会（以下简称密评联委会），聚焦密评人才队伍教育与培训、密评相关标准制定、密评技术评价和能力评估、密评关键共性技术研究、密评行业发展促进等重点工作。2021 年 11 月，国家密码管理局印发《关于规范商用密码应用安全性评估结果备案工作的通知》（国密局字〔2021〕392 号），明确



规范商用密码应用安全性评估结果备案相关要求，密评体系进一步规范。2023 年 7 月，《商用密码管理条例》正式施行，设立专章推进商用密码检测认证体系建设，密评体系逐步走向完善。

2.1 密评工作机制

密评工作主要涉及的主体有密码管理部门、行业主管部门、商用密码应用安全性评估机构（以下简称密评机构）、网络运营者以及密评联委会等。按照《商用密码管理条例》《商用密码应用安全性评估管理办法（征求意见稿）》《商用密码检测机构管理办法（征求意见稿）》《关于规范商用密码应用安全性评估结果备案工作的通知》（国密局字〔2021〕392 号）、《关于进一步规范商用密码应用安全性评估试点工作的通知》（国密局字〔2022〕454 号）等法规文件要求，以上各主体在密评工作中的职责如下。

2.1.1 国家密码管理部门负责管理全国的商用密码工作

一是负责和有关部门建立商用密码监督管理协作机制，加强商用密码监督、检查、指导等工作的协调配合。
二是负责全国商用密码检测机构的资质认定和监督管理；负责管理全国的商用密码应用安全性评估工作。
三是规范商用密码应用安全性评估结果备案工作，并对密评结果备案材料进行季度抽查并组织开展技术复核，定期通报各地区密评结果备案材料形式审查工作成效和技术复核结果。

2.1.2 地方各级密码管理部门负责管理本行政区域的商用密码工作

一是县级以上地方各级密码管理部门负责本行政区域内商用密码检测机构的监督管理；负责管理本行政区域的商用密码应用安全性评估工作。
二是县级以上地方各级密码管理部门负责督促本地区有关网络运营者同步规划、同步建设、同步运行商用密码保障系统，规范开展密评工作。
三是各省、自治区、直辖市密码管理部门负责指导本地区有关网络运营者履行备案程序，并对备案材料进行形式审查；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。

2.1.3 行业主管部门推动本行业本领域密码应用

一是和密码管理部门建立商用密码监督管理协作机制，加强商用密码监督、检查、指导等工作的协调配合，推进重要领域和行业商用密码应用。
二是在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。
三是采取多种形式加强商用密码宣传教育，增强公民、法人和其他组织的密码安全意识。

2.1.4 密评机构开展商用密码应用安全性评估具体实施

密评机构是商用密码检测机构的一类，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。

一是按照法律、行政法规和商用密码检测技术规范、规则，在批准范围内独立、公正、科学、诚信地开展商用密码检测，对出具的检测数据、结果负责。

二是对检测原始记录和检测报告归档留存，保证其具有可追溯性。原始记录和检测报告的保存期限不得少于 6 年。

三是于每年 1 月 15 日前通过所在地省、自治区、直辖市密码管理部门向国家密码管理局报送上一年度工作报告以及相关统计数据。

四是积极配合密码管理部门的监督检查，如实提供相关材料和信息。

商用密码检测机构及相关从业人员应当按照法律法规、标准规范等要求开展检测活动，遵循客观独立、科学公正、诚实信用原则，尊重知识产权，恪守职业道德，承担社会责任，保守在工作中知悉的国家秘密、商业秘密和个人隐私。

2.1.5 网络运营者履行密评主体责任

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关键信息基础设施、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，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。

一是在系统规划阶段，网络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。

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。

二是在系统建设阶段，网络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。

系统运行前，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。

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影响，并需提供如下支持：

- （1）对网络与信息系统的重要数据进行备份；
- （2）提供完整有效的网络与信息系统设备清单和网络拓扑；
- （3）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；
- （4）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；
- （5）安排网络与信息系统相关网络管理员、系统管理员、商用密码产品管理员等做好配合；
- （6）其他需要配合的事项。

三是系统建成运行后，网络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。

四是网络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，必要时启动应急处置方案并开展商用密码应用安全性评估。

网络运营者应当在商用密码应用安全性评估报告出具之日起 30 日内，将评估报告连同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。

2.1.6 密评联委会支撑密评各项工作开展

商用密码领域的学会、行业协会等社会组织依照法律、行政法规及其章程的规定，开展学术交流、政策研究、公共服务等活动，加强学术和行业自律，推动诚信建设，促进行业健康发展。在国家密码管理局的指导下，密评联委会全面支撑密评人才队伍教育与培训、标准制定、技术评价和能力评估、关键共性技术的研究、密评行业促进等方面工作。

一是依托密码行业标准化技术委员会（以下简称密标委），推动商用密码应用与安全性评估标准规范制定。规划设计密评标准体系，提出标准编制需求、发布编制任务、征集编制单位、与密标委对接完成标准立项、推进研制、质量把关、标准验证、标准修订等，以及标准配套指导性文件的跟踪研究及制修订工作。组织开展标准宣贯、解读及相关培训、研讨活动，主动了解行业密码应用需求，推进行业相关标准制定或内容嵌入。

二是支撑密码管理部门建立密评机构能力验证体系，完善配套流程机制，明确密评机构能力综合评价和理论考试、技能考核、报告质量评价等具体环节的方法与指标，并支持搭建密评能力验证实训环境。支撑密码管理部门建立完善密评人员培训考核体系，开展密评人员水平评价。

三是推动密评行业自律建设及宣贯推广。负责制定并组织实施密评行业自律公约，规范密评机构市场竞争及密评过程行为等。建立密评行业信息收集、反馈、通报机制，促进行业信息公开，支撑建立密评行业信息平台，加强密评工作信息发布与宣传推广。通过学术研讨、专题论坛、技术沙龙、专业讲座及知识竞赛等方式，提升密评队伍的综合素养和专业能力，加强密评经验交流与创新研究。

2.2 密评机构培育

作为密评试点工作的重要内容，机构培育与密评开展相辅相成，日益壮大的密评队伍力量支撑着密评工作的健康持续发展。国家密码管理局按照“总量控制、合理布局、择优选择”原则，采取“省部推荐、集中考核”模式，于 2017 年 4 月、2019 年 9 月分两批培育认定密评试点机构并进行分类管理，其中 48 家纳入《商用密码应用安全性评估试点机构目录》并面向社会公布，可在全国范围内开展密评工作，25 家准予在本地区、本行业从事密评工作，覆盖全国 26 个省（自治区、直辖市）、11 家部委或央企行业领域。

随着《商用密码管理条例》正式施行，密评机构作为商用密码检测机构的一类，具备了行政许可的基础。国家密码管理局积极组织制修订《商用密码检测机构管理办法》《商用密码应用安全性评估管理办法》等配套规章，推动落实密评机构行政许可，为密评依法管理提供基础。随着管理模式由试点资格向许可资质过渡，密评机构层次范围、质量水平将得到进一步提升拓展。

2.3 密评系列标准

自 2017 年密评试点工作启动以来，国家密码管理局持续加强密评标准规范供给。试点工作之初，研究确定了密评体系总体架构，并组织有关单位起草 14 项制度文件，明确了密评体系建设、密评机构培育、密评活动开展的基本依据。近年来，在国家密码管理局的指导下，相关标准化组织及密评联委会立足密评试点工作实际，积极组织密评标准及指导性文件制修订工作，推动密评工作标准化建设，为密评活动有序开展搭建标准化支撑基础。

2.3.1 密评系列标准框架

随着密评试点工作的深入，密评系列标准不断完善。GM/T 0054-2018《信息系统密码应用基本要求》（以下简称 GM/T 0054-2018）从行业标准上升为国家标准 GB/T 39786-2021《信息安全技术 信息系统密码应用基本要求》（以下简称 GB/T 39786-2021），为密评工作开展提供基础性指导。密码行业标准 GM/T 0115-2021《信息系统密码应用测评要求》（以下简称 GM/T 0115-2021）、GM/T 0116-2021《信息系统密码应用测评过程指南》（以下简称 GM/T 0116-2021）以及指导性文件《商用密码应用安全性评估量化评估规则》《信息系统密码应用高风险判定指引》等相继发布，规范了测评要求、测评过程、测评结果以及测评报告等内容。截至目前，已有 1 项商用密码应用与安全性评估相关国家标准发布、2 项在研，2 项相关密码行业标准发布、4 项在研，5 项指导性文件发布。

商用密码应用安全性评估相关标准经历了从无到有、不断优化的过程，逐步构建了涵盖应用类、评估类和管理类的密评系列标准框架（如图 1 所示）。应用类标准指导信息系统商用密码应用，同时也是评判密码应用是否合规的依据；评估类标准依据应用类标准制定，具体指导密评工作的开展；管理类标准是密评工作的基础和保障。这些标准和指导性文件相互关联、相互支撑，有力支撑了《密码法》和《商用密码管理条例》的落地实施。

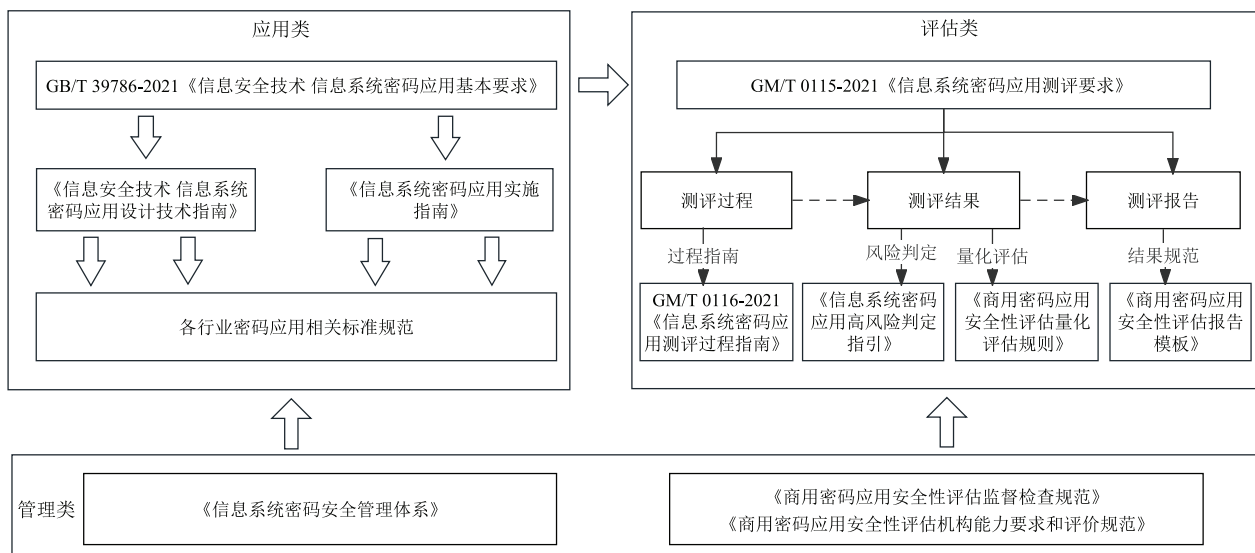


图 1 密评系列标准示意图



2.3.2 密评系列标准主要内容

(1) GB/T 39786-2021 为密评工作提供基础性指导

GB/T 39786-2021 用于指导、规范信息系统密码应用的规划、建设、运行及测评，是指导密评工作开展的基础性标准。该标准规定了信息系统从第一级到第四级的密码应用的基本要求，从信息系统的物理和环境安全、网络和通信安全、设备和计算安全、应用和数据安全四个方面提出了密码应用技术要求，从管理制度、人员管理、建设运行和应急处置四个方面提出了密码应用管理要求。在该标准的基础上，各领域与行业可结合本领域与行业的密码应用需求来指导、规范信息系统密码应用。

同时，密评试点的具体实践和工作经验对 GB/T 39786-2021 的编制起到了积极的促进作用。2018 年 9 月 26 日，该标准项目组在国家密码管理局和全国信息安全标准化技术委员会 WG3 工作组的指导下，向全国 27 家密评试点机构征求意见。2018 年 9 月到 10 月，该标准项目组根据 27 家密评试点机构的意见，对标准进行了多次研讨，将身份鉴别、访问控制、数据完整性等部分条款进行调整与修改。来自真实应用场景的密评试点实践成果有力支撑了 GB/T 39786-2021 的编制工作，相较于标准前身密码行业标准 GM/T 0054-2018，国标 GB/T 39786-2021 的合理性和可操作性得到进一步提升。

(2) 密评相关标准及指导性文件有力支撑密评工作开展

近年来，在国家密码管理部门的指导下，我国陆续出台了一系列商用密码应用与安全性评估相关标准规范与指导性文件，主要涉及信息系统密码应用设计、建设、测评等各工作环节的要求。密评系列标准包含应用、评估及管理三类标准。

表 4 密评相关标准及指导性文件

类别	标准及指导性文件名称	状态	主要内容
应用类	《信息安全技术 信息系统密码应用设计技术指南》	在研	包括信息系统密码应用框架、密码应用方案设计原则、密码应用方案设计过程和密码应用方案设计指南，适用于指导信息系统密码应用方案的设计，也可作为信息系统密码保障系统建设、密码应用安全性评估、密码管理部门密评备案工作的参考。
	《信息系统密码应用实施指南》	在研	参照 GB/T 39786-2021 给出了信息系统密码应用的过程指导和建议，描述了规划、建设、运行及终止阶段的实施流程及主要活动，适用于指导信息系统密码应用的实施。
评估类	GM/T 0115-2021 《信息系统密码应用测评要求》	发布	规定了信息系统不同等级密码应用的测评要求，从密码算法、密码技术、密码产品和密码服务合规性、密钥管理安全性方面，提出了第一级到第五级的密码应用通用测评要求；从信息系统的物理和环境安全、网络和通信安全、设备和计算安全、应用和数据安全等四个技术层面提出了第一级到第四级密码应用技术的测评要求；从管理制度、人员管理、建设运行和应急处置等四个管理方面提出了第一级到第四级密码应用管理的测评要求，并给出了整体测评、风险分析和评价、测评结论等测评环节的要求。该标准适用于指导、规范信息系统在规划、建设、运行环节的密评工作。该标准升国标的工作正在进行。
	GM/T 0116-2021 《信息系统密码应用测评过程指南》	发布	规定了信息系统密码应用的测评过程。该标准在遵循测评的客观公正性原则、可重用性原则、可重复性和可再现性原则及结果完善性原则的基础上，规范了各项测评活动及其工作任务。

类别	标准及指导性文件名称	状态	主要内容
评估类	《商用密码应用安全性评估量化评估规则》	发布	依据 GB/T 39786-2021 和 GM/T 0115-2021 对信息系统的密码应用情况给出定量评估结果，适用于规范信息系统密码应用安全性评估，以及指导相关信息系统的规划、建设等工作。该指导性文件结合当前密码应用推进的实际情况，鼓励网络运营者使用密码技术，特别是使用合规的密码技术、产品和服务，并且优先在网络和通信安全层面、应用和数据安全层面推进商用密码应用。
	《信息系统密码应用高风险判定指引》	发布	给出了信息系统密码应用过程中可能存在的高风险安全问题，强调密评过程要按照“综合判定、保住底线”的思路，一定程度上既保证信息系统具备安全防护能力，又有利于促进信息系统的密码应用，强调密码产品、密码服务自身的安全性，引导网络运营者使用合规的密码产品和服务，防止因产品和服务问题给系统带来新的风险。
	《商用密码应用安全性评估报告模板》（2023 版）	发布	包括《商用密码应用安全性评估报告模板（2023 版）—方案密评报告》报告模板（以下简称方案密评报告模板）和《商用密码应用安全性评估报告模板（2023 版）—系统密评报告》模板（以下简称系统密评报告模板）。方案密评报告模板对信息系统密码应用方案的密评报告格式进行了规范，系统密评报告模板对信息系统的密评报告格式进行了规范。
	《商用密码应用安全性评估 FAQ》	发布	以问答形式解释了密评过程中常见的典型问题，为相关单位和从业人员开展密评工作提供参考。确立了定期更新机制，不断应对技术发展和应用情况的变化，以持续保持密评标准体系的活力。
	《信息安全技术 信息系统密码应用测评要求》	在研	根据 GB/T 39786-2021，将信息系统密码应用测评要求分为通用测评要求和密码应用测评要求，规定了信息系统不同等级密码应用的测评要求，从密码算法、密码技术、密码产品和密码服务合规性、密钥管理安全性方面，提出了第一级到第五级的密码应用通用测评要求；适用于指导、规范信息系统密码应用在规划、建设、运行环节的商用密码应用安全性评估工作。
管理类	《商用密码应用安全性评估机构能力要求和评价规范》	在研	规定了密评机构的能力要求和评价规范。在密评机构能力要求方面，具体给出了基本条件、组织管理要求、资源要求（人员、工作场所条件、设施与设备、分包等）、风险控制能力要求、质量管理要求；在密评机构能力评价方面给出了评价流程、初次评价、期间评价、能力复评等要求。
	《商用密码应用安全性评估监督检查规范》	在研	规定了商用密码应用安全性评估监督检查工作的组织管理形式、监督检查对象、检查工作内容和实施开展方式，为国家密码管理部门和省（市）密码管理部门对辖内机构实施日常监督检查提供依据，为重要领域网络和信息系统建设、使用、管理单位进行商用密码应用自查工作提供标准，为密评机构实施密评工作提供合规性指导。
	《信息系统密码安全管理体系》	在研	参考 GB/T 22080《信息技术 安全技术 信息安全管理体系要求》，在 GB/T 39786-2021 的基础上，结合国内密码应用安全管理和实践经验进行制定，为网络运营者建立组织内部的密码应用安全管理体系提供指导。标准内容包括管理保障、密码应用安全风险、密码应用安全控制、有效性测量、持续改进和密码应用安全管理体系评估等。

2.3.3 密评标准的特点

在国家密码管理部门的指导下，密评相关标准规范、指导性文件在规范密评活动的同时，也在密评试点过程中得到验证和完善。



一是注重与相关标准的衔接性与协调性。《中华人民共和国密码法》第二十七条明确要求“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、网络安全等级测评制度相衔接,避免重复评估、测评。”密评相关标准在制修订过程中严格落实法律要求,并注重密评与关键信息基础设施安全检测评估、网络安全等级测评工作衔接。以 GB/T 39786-2021 为例。

第一, GB/T 39786-2021 是商用密码应用安全性评估的基础性指导。GB/T 39786-2021 和 GB/T 22239-2019《信息安全技术 网络安全等级保护基本要求》(以下简称 GB/T 22239-2019)二者既相互补充,又可相互独立实施。标准内容的合理设计,有效避免了网络安全等级保护测评、密评工作在实施过程出现重复评估、测评的情况。

第二,信息系统遵循的密码应用等级及范围参照网络安全等级保护定级。信息系统根据 GB/T 22240-2020《信息安全技术 网络安全等级保护定级指南》完成定级备案后,其密码应用等级及范围也相应确定。从密评机构的视角看,信息系统完成等级保护定级是启动密评的基础,密评对象的范围与等级保护定级范围保持一致,以减少密评对象等级不同所带来的复杂性。

第三,在标准具体条款内容上,注意与关键信息基础设施安全检测评估、网络安全等级测评相关标准规范内容的一致性。例如,在 GB/T 22239-2019 中,对于等级保护第三级系统的数据完整性要求是“应采用校验技术或密码技术”保障完整性,对于等级保护第四级系统提出“应采用密码技术”保障完整性。因此,在 GB/T 39786-2021 制定过程中,将对应行标 GM/T 0054-2018《信息系统密码应用基本要求》第三级中对完整性要求的约束程度由“应”调整为 GB/T 39786-2021 中的“宜”,第四级维持“应”的要求。

第四, GM/T 0115-2021《信息系统密码应用测评要求》、GM/T 0116-2021《信息系统密码应用测评过程指南》是为配合 GB/T 39786-2021 的贯彻实施,更好地指导和规范密评工作而制定的两部行业标准,相关标准规范制定中注意与现行法律、法规以及国家标准相衔接,保证标准规范内容的合规性。

二是标准制定具有科学性与可落地性。在密评试点推进伊始,对信息系统密码应用安全性评估的结果判定采用符合性判定“一票否决”的机制,但随着密评工作的推进,该机制的不适应性逐步显现。一方面,密码应用推进工作难度大、周期长,“一票否决”不利于网络运营者统筹各方资源落实密码应用要求。另一方面,密评机构在实施标准过程中,缺乏量化评分机制,评估过程和评估结果缺乏说服力。

结合密码应用推进工作实际,《商用密码应用安全性评估量化评估规则》《信息系统密码应用高风险判定指引》制定工作适时启动,目前以指导性文件的形式在实际工作中使用,起到了较好的规范和引领作用。相比于原有“一票否决”的规则,“量化评估+风险判定”的综合判定思路完善了密评结果的出具过程。量化评估是为了“保量”,即商用密码应用应当达到一定的程度,便于纵向和横向的比较;风险判定是为了“保质”,即守住信息系统的安全底线。

在风险可控前提下,《商用密码应用安全性评估量化评估规则》对系统的密码应用情况给出科学的定量评价指标,主要从密码使用有效性、密码算法/技术合规性、密钥管理安全三个方面量化评估。密码使用有效性关注密码技术是否被正确、有效使用,以满足信息系统的安全需求。密码算法/技术合规性关注信息系统使用的密码算法是否符合法律、行政法规、国家有关规定和密码相关国家标准、行业标准的要求,密码技术是否遵循密码相关国家标准和行业标准或通过国家密码管理部门审查鉴定。密钥管理安全关注密钥管理的全生命周期是否安全,用于密码计算或密钥管理的密码产品、密码服务是否安全。

随着全社会密码应用保障系统的建设和能力的提高，量化评估阈值也会随之进行调整。密码应用安全的量化评估不仅有助于呈现密码应用推进的阶段性成果，而且为密码应用安全持续改进指明了方向。

三是标准制修订具备灵活性与适应性。密评活动离不开密码应用保障系统的建设情况，制修订密评标准规范既要保证一定的先进性，又要结合实际情况，确保标准规范真正起到指导密评活动正常有序开展的作用。随着试点工作的不断推进，密评系列标准也在不断丰富和发展。

第一，在试点阶段，为了更好地指导和规范密评机构开展密评工作，密评联委会本着“共性先立、急用先行”的原则，通过指导性文件的方式先行发布一些亟需规范。2020年密评联委会发布《信息系统密码应用测评要求》等5项商用密码应用与安全性评估指导性文件，之后，多次更新发布了《信息系统密码应用高风险判定指引》《商用密码应用安全性评估量化评估规则》《商用密码应用安全性评估报告模板》等指导性文件。

第二，在密码行业标准层面积极推动密评标准制定，同时，对基础性的、需要在全国范围内统一的技术要求，适时启动行标升国标或国标编制的工作，如GB/T 39786-2021《信息安全技术 信息系统密码应用基本要求》、正在制定的国标《信息安全技术 信息系统密码应用测评要求》。

第三，持续推进标准文件更新出台，不断为密评标准注入生命力。一方面，密码应用与安全性评估活动越来越频繁，亟需规范的活动内容越来越多。另一方面，密码应用场景的不断丰富，对不同场景、不同行业应用系统的密评工作带来了新的挑战。因此，需要积极归纳总结密评试点过程的宝贵经验，根据不同场景和典型业务需求丰富完善相关标准内容。在后续工作中，结合试点实践情况，还需要进一步推进指导性文件加快成熟，并适时制定发布相应的标准文件，以更好地指导商用密码应用与安全性评估工作。

2.4 密评程序

密评开展程序如图2所示，在系统规划阶段、建设阶段、运行阶段，网络运营者和密评机构需紧密配合，完成密码应用方案评估和信息系统密评工作，并将评估结果报密码管理部门备案。

在系统的规划阶段，网络运营者应当依照相关法律法规和标准规范，自行或组织商用密码相关单位，根据网络安全等级保护定级情况和密码应用需求，依据GB/T 39786-2021等相关标准要求制定商用密码应用方案，规划商用密码保障系统。方案编制完成后，自行或者委托商用密码检测机构开展密码应用方案商用密码应用安全性评估。密码应用方案未通过密评的，不得作为商用密码保障系统的建设依据。

在系统的建设阶段，网络运营者自行或组织相关商用密码产业单位、系统开发商等支撑单位，按照通过商用密码应用安全性评估的商用密码应用方案进行实施，落实商用密码安全防护措施，建设商用密码保障系统。系统运行前，网络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。系统未通过商用密码应用安全性评估的，针对评估中发现的安全问题及时整改，整改完成后可请密评机构进行复评，改造期间不得投入运行。仍未通过的，不得通过项目验收。

在系统建成运行后，网络运营者应当按照法律法规等相关要求，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。系统发生密码相关重大安全事

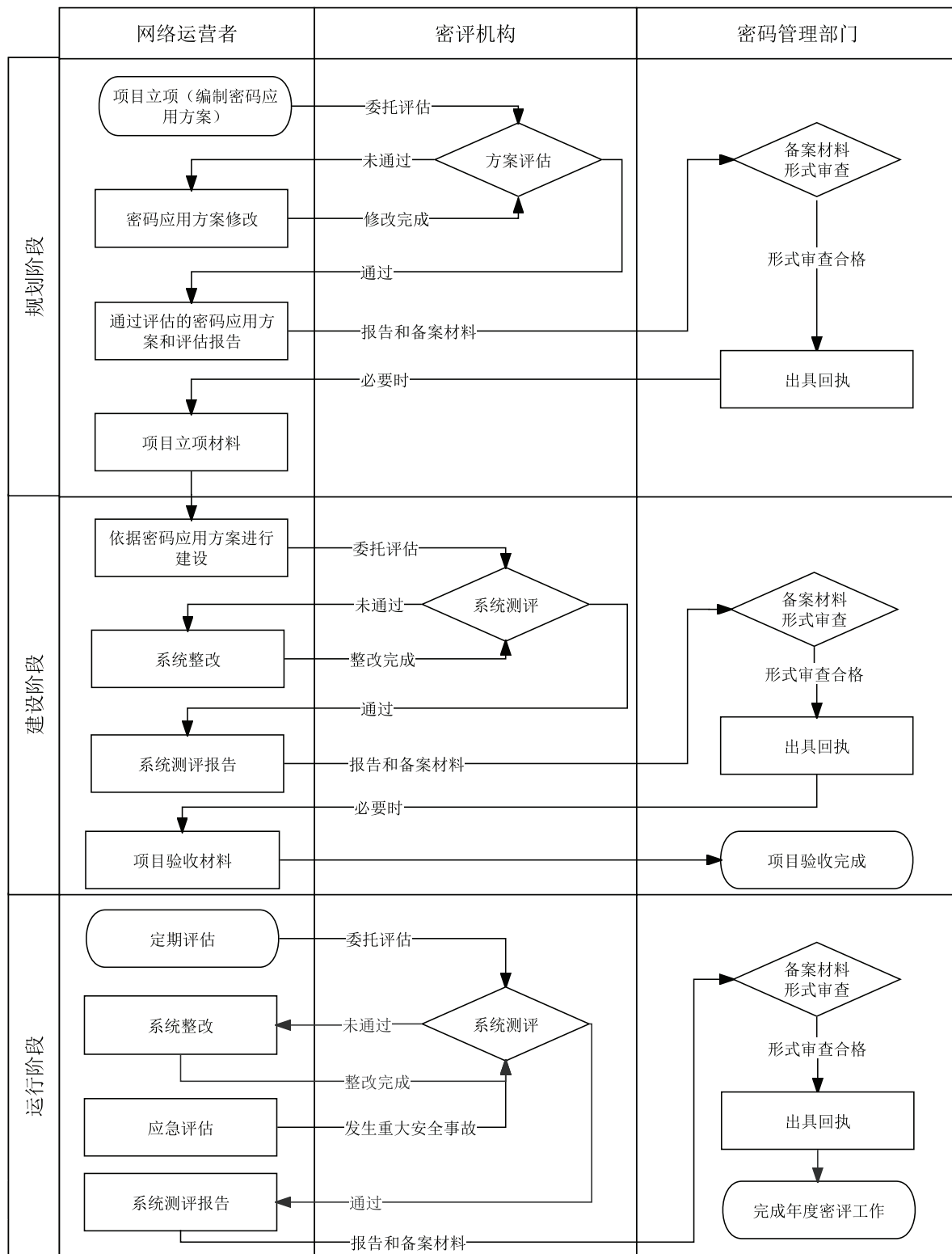


图 2 密评程序

件、重大调整或特殊紧急情况时，网络运营者应当及时联系商用密码检测机构开展商用密码应用安全性评估，并依据评估结果进行应急处置，采取必要的安全防范措施。未通过商用密码应用安全性评估的，网络运营者应当进行改造。若系统约束条件发生重要变化，必要时，项目使用单位需重新修订和编制密码应用方案，对系统进行升级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。

完成规划、建设、运行和应急评估的每一个阶段时，网络运营者应当在商用密码应用安全性评估报告出具 30 日内，填写《网络与信息系统密评备案信息表》等密评工作情况相关材料，按照国家密码管理部门有关规定，连同评估报告一起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应当对备案材料进行形式审查，审查不通过的，应当责令网络运营者重新提供商用密码应用安全性评估报告。相关商用密码检测机构应当配合网络运营者重新开展商用密码应用安全性评估或者重新出具商用密码应用安全性评估报告，不得重复收取费用。

3

密评行业发展情况

3.1 密评试点机构规模布局日趋合理

2021 年国家密码管理局公告（第 42 号）发布的密评试点机构共 48 家，可在全国范围内开展密评工作。48 家密评试点机构覆盖全国 18 个省（自治区、直辖市），其中行业主管部门推荐机构 20 家，地方密码管理部门推荐机构 28 家，如图 3 所示。地方密码管理部门推荐的 28 家机构中，北京市、浙江省、广东省各 3 家，上海市、山东省、四川省、新疆维吾尔自治区各 2 家，天津市、河北省、辽宁省、吉林省、江苏省、安徽省、福建省、江西省、河南省、湖南省、重庆市各 1 家。

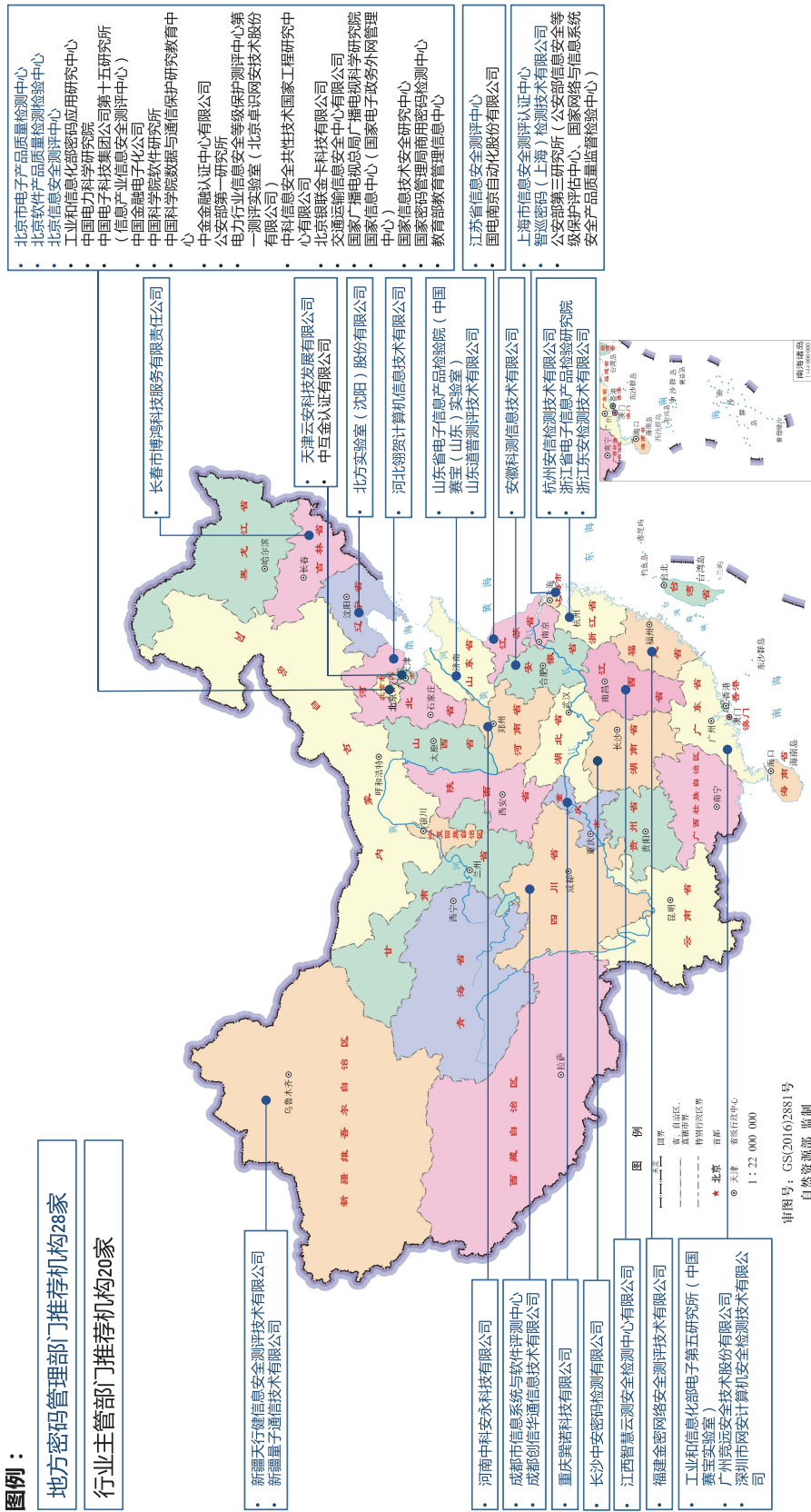


图 3 密评试点机构布局分布

3.2 密评人才供给能力持续提升

近年来，密码专业人才培养质量和数量“双提升”。国家密码管理局持续加大密评从业人员考核力度，先后于2017年11月、2020年1月、2022年7月、2023年7月组织4次密评人员考核，通过密评人员考核人数稳步增加，为密评工作开展提供了重要的人才保障。2021年3月，“密码科学与技术”列入《普通高等学校本科专业目录（2021年）》，高等职业教育专科专业增加“密码技术应用”专业。2022年9月，密码专业正式纳入《研究生教育学科专业目录（2022年）》。目前已有15所高校开设“密码科学与技术”本科专业。2022年9月，人力资源社会保障部颁布了2022版《中华人民共和国职业分类大典》，新增“密码技术应用员”和“密码工程技术人员”两个职业。密码技术应用员定义为从事信息系统安全密码保障的架构设计、系统集成、检测评估、运维管理、密码咨询等相关密码服务的人员。密码工程技术人员定义为从事密码算法与协议实现、设备和系统研制、产品检测与认证、服务系统设计建设、标准编制、密码管理、专业技术培训咨询的工程技术人员。《密码技术应用员国家职业技能标准》《密码工程技术人员国家职业标准》均已公开发布，密码职业人才培养认定体系正加速构建，可有效满足密评人才需求。

3.3 密评覆盖范围逐年扩大

密评试点启动至今，密评服务领域覆盖范围越来越广，覆盖电子政务、金融、公安、能源、卫生健康等重点领域。2018-2022年，年度开展系统评估的系统数量从81个增长到4665个，实现了大幅增长。



按照区域划分，2018-2022 年各区域开展密评数量的统计如表 5 及图 4 所示。各区域密评数量基本呈上升趋势，华东地区密评数量在各区域中排名第一。

表 5 各区域开展密评数量统计表

地区	华北	东北	华东	华中	华南	西南	西北
2018 年数量	41	2	15	5	6	7	5
2019 年数量	115	68	97	114	72	56	40
2020 年数量	62	18	174	31	88	142	15
2021 年数量	237	133	512	118	195	443	192
2022 年数量	886	202	1173	402	791	726	485
总数	1341	423	1971	670	1152	1374	737

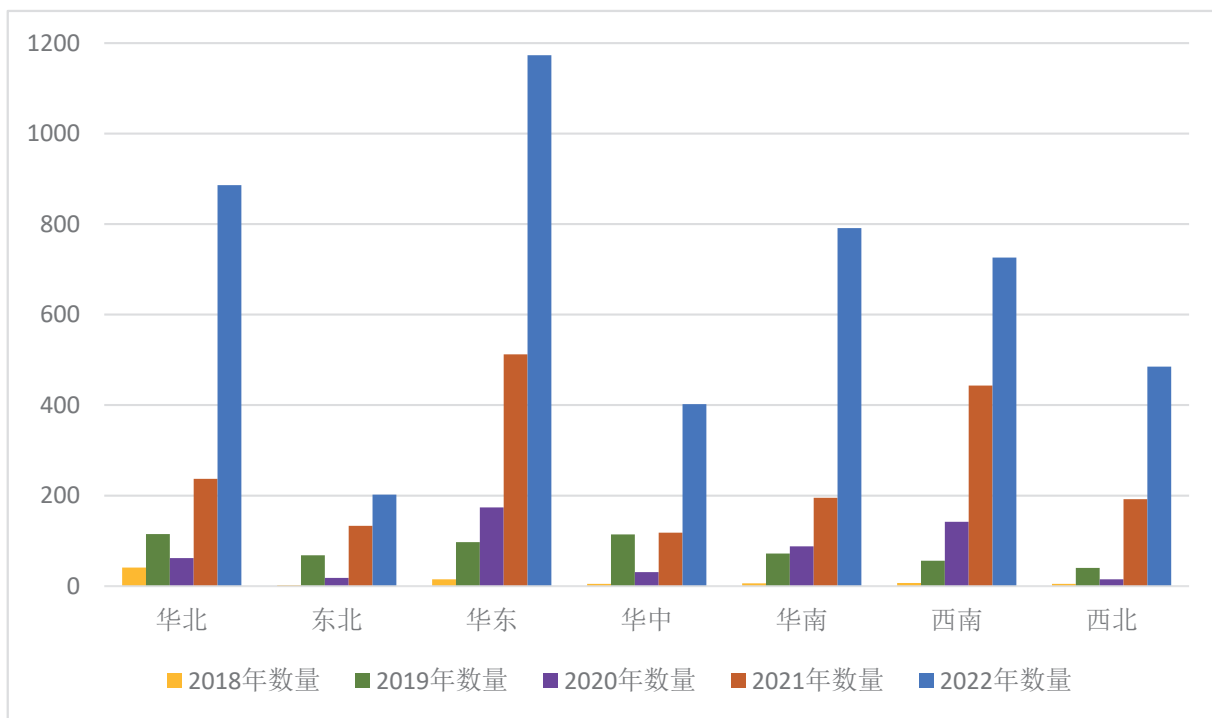


图 4 各区域密评数量统计图

按照系统所属行业领域划分，2018-2022 年各行业开展密评数量的统计如表 6 及图 5 所示。各行业密评数量基本呈上升趋势，政务行业密评数量在各行业中排名第一。

表 6 各行业密评数量统计表

行业	政务	金融	公安	能源	卫生健康	社会保障	自然资源	交通	其他
2018 年数量	19	15	7	5	3	5	2	7	18
2019 年数量	209	75	29	26	32	26	15	44	106
2020 年数量	172	24	92	74	36	19	14	52	47
2021 年数量	830	163	199	104	112	133	53	74	162
2022 年数量	2002	434	380	498	337	210	261	146	397
总数	3232	711	707	707	520	393	345	323	730

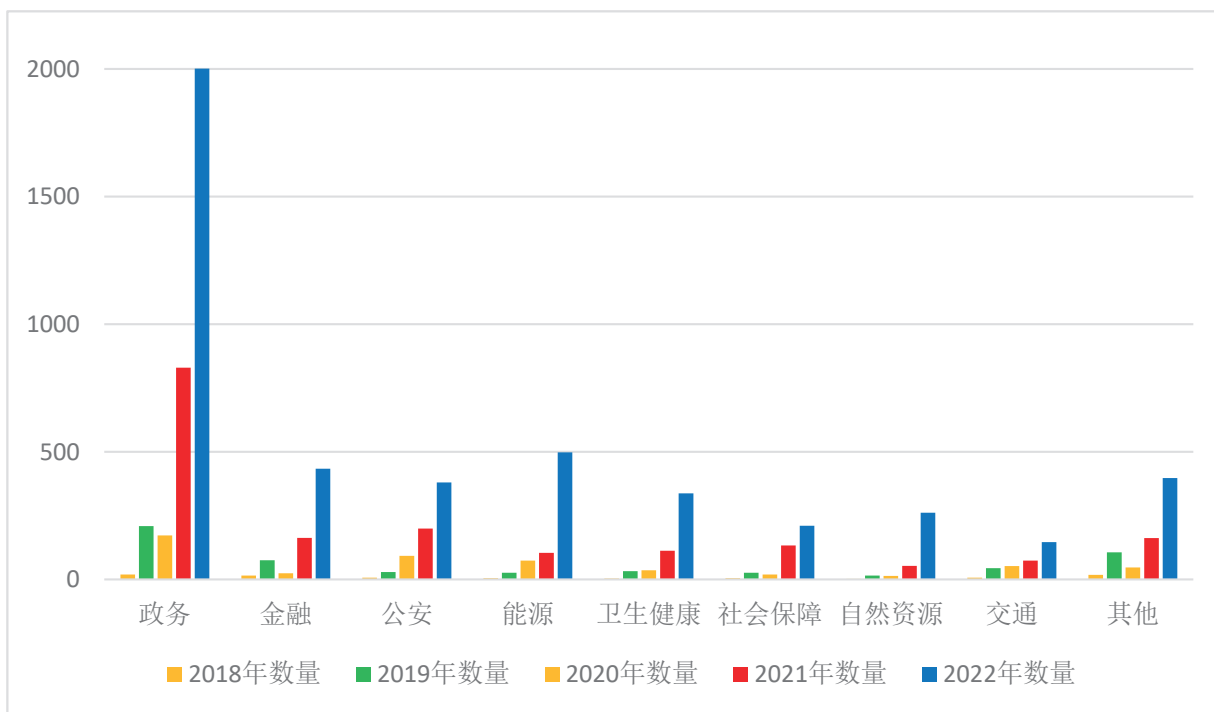


图 5 各行业密评数量统计图



2018-2022年各年度密评结论统计如图6所示,从密评结果来看,各年度密评通过率呈现逐年增长的趋势。

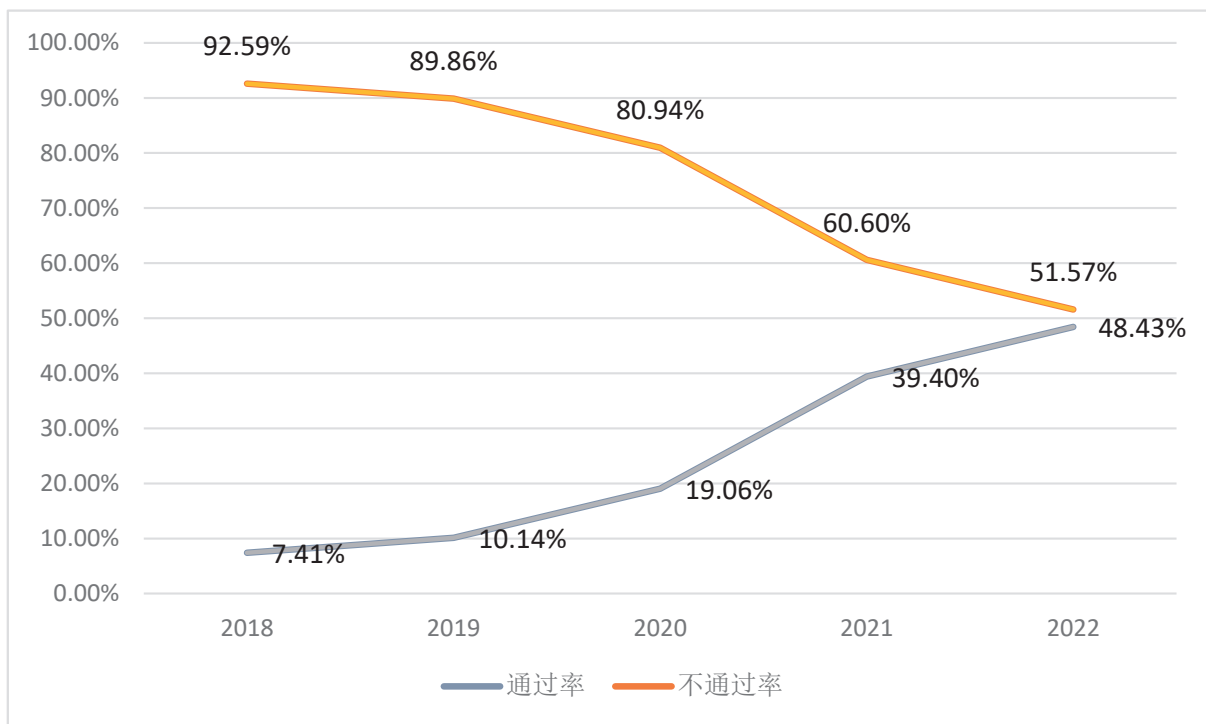


图6 各年度密评通过 / 不通过率统计图

按照机构划分,2018-2022年各年度机构开展密评数量(前十)的统计如图7所示。

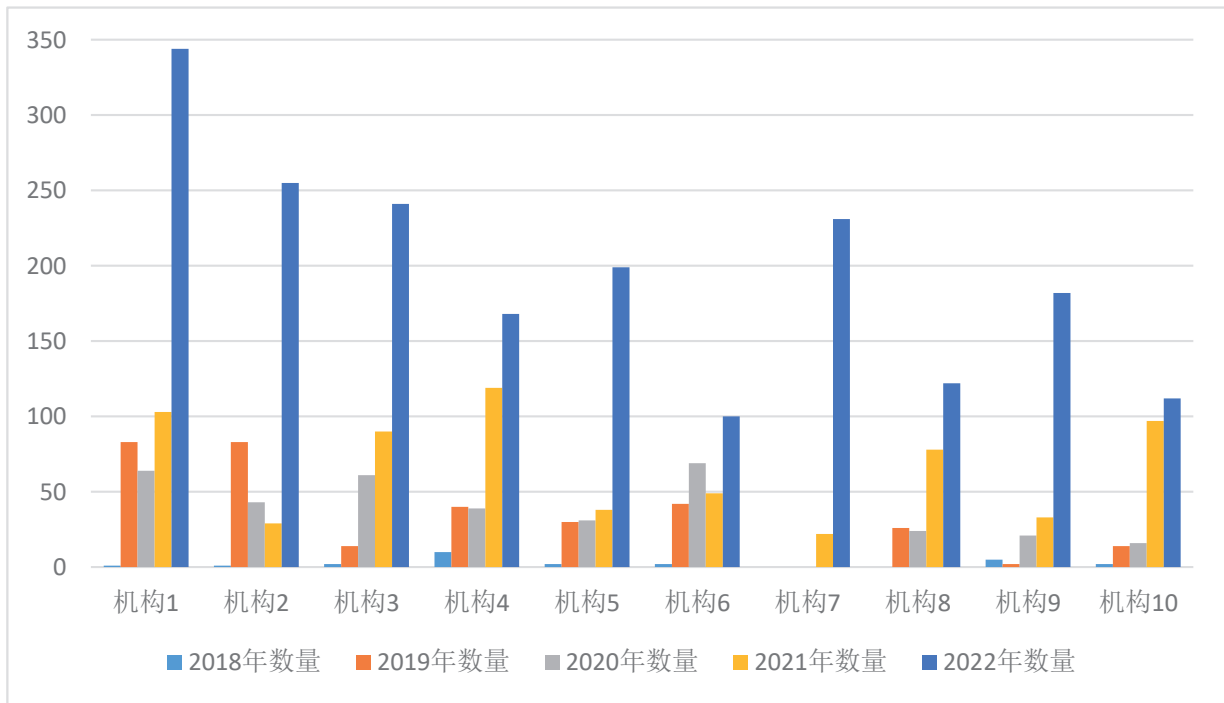


图7 各年度机构密评数量(前十)统计图

4

发展建议

外部支撑体系建立健全，密评发展根基持续夯实。加快推进《商用密码管理条例》配套制度出台实施，推动商用密码应用安全性评估要求与各地区各有关部门相关工作规划及政策制度同步部署、深度融合、配套落地，统筹建立资金、人员、技术等方面要素保障机制与参考依据，形成制度化、常态化、便利化安排，实现密评工作与网络化、数字化发展战略深度融合。加强密码宣传教育与密评引导培训，为密码应用单位在信息系统规划、建设、运行、管理各环节提供密评政策支持和操作指导。

内在实施要素供给稳定充足，适应数字经济发展的密评事业有利局面逐步形成。系统完善密评相关国家标准、行业标准、团体标准，推出密评相关问题库、知识库与案例库，以及面向大数据、物联网、人工智能、云计算、车联网、区块链、隐私计算等新领域、新场景、新技术的技术指南与测评规范，不断增加场景化实施要素，提升密评可操作性与落地性。强化密评管理平台、工具、手段创新，研究建设密码运行安全管理基础设施，实现密评监管在线化、动态化、实时化，推动密评决策信息化、精准化、科学化，通过提升管理效能可为行业生态建设添砖加瓦。

依法管理有力实施，规范有序的密评市场活力充分激发。规范密评市场秩序，落实密评结果备案等管理制度，组织开展密评工作“飞行检查”，严厉查处密评违法违规行为。健全密评联委会组织体系，有效整合密评机构参与力量，探索引入社会监督，围绕密评行业总体规划、标准供给、能力建设、行业自律等方面广泛吸纳智慧方案。加强各地区各部门各机构密评实践定向指导、经验交流与督促考核，全力推动密评机构由试点管理向行政许可衔接转换，建立密评机构常态化准入及退出机制，加快实现密评职业人才常态化教育培训及社会化评价认定，丰富机构队伍及专业人才供给。



附录 1：密评相关法规政策汇总

1.1 国家层面密码应用及密评相关法律法规

发文/ 起草单位	发布/ 施行时间 (注：已发布法律法规为“施行时间”，其他为“发布时间”)	政策文件	相关内容
第十三届全国人民代表大会常务委 员会第十四次会议通过	2020 年 1 月 1 日	《密码法》 (中华人民共和国主席令第三十五号)	第二十七条：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关键信息基础设施，其运营者应当使用商用密码进行保护，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。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、网络安全等级测评制度相衔接，避免重复评估、测评。 关键信息基础设施的运营者采购涉及商用密码的网络产品和服务，可能影响国家安全的，应当按照《中华人民共和国网络安全法》的规定，通过国家网信部门会同国家密码管理部门等有关部门组织的国家安全审查。
第十二届全国人民代表大会常务 委员会第二十四次会议通过	2017 年 6 月 1 日	《网络安全法》 (中华人民共和国主席令第五十三号)	第十条：建设、运营网络或者通过网络提供服务，应当依照法律、行政法规的规定和国家标准的强制性要求，采取技术措施和其他必要措施，保障网络安全、稳定运行，有效应对网络安全事件，防范网络违法犯罪活动，维护网络数据的完整性、保密性和可用性。 第二十一条：采取数据分类、重要数据备份和加密等措施。
第十三届全国人民代表大会常务 委员会第二十九次会议通过	2021 年 9 月 1 日	《数据安全法》 (中华人民共和国主席令第八十四号)	第二十七条：开展数据处理活动应当依照法律、法规的规定，建立健全全流程数据安全管理制度，组织开展数据安全教育培训，采取相应的技术措施和其他必要措施，保障数据安全。利用互联网等信息网络开展数据处理活动，应当在网络安全等级保护制度的基础上，履行上述数据安全保护义务。
第十三届全国人民代表大会常务 委员会第三十次会议通过	2021 年 11 月 1 日	《个人信息保护法》(中华人民共和国主席令第九十一号)	第五十一条：个人信息处理者应当根据个人信息处理目的、处理方式、个人信息的种类以及对个人权益的影响、可能存在的安全风险等，采取下列措施确保个人信息处理活动符合法律、行政法规的规定，并防止未经授权的访问以及个人信息泄露、篡改、丢失： …… (三) 采取相应的加密、去标识化等安全技术措施。

发文 / 起草单位	发布 / 施行时间 (注:已发布法律法规为“施行时间”,其他为“发布时间”)	政策文件	相关内容
国务院第4次常务会议修订通过	2023年4月14日	《商用密码管理条例》	第三十八条: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关键信息基础设施,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,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。 前款所列关键信息基础设施通过商用密码应用安全性评估方可投入运行,运行后每年至少进行一次评估,评估情况按照国家有关规定报送国家密码管理部门或者关键信息基础设施所在地省、自治区、直辖市密码管理部门备案。 第四十一条:网络运营者应当按照国家网络安全等级保护制度要求,使用商用密码保护网络安全。国家密码管理部门根据网络的安全保护等级,确定商用密码的使用、管理和应用安全性评估要求,制定网络安全等级保护密码标准规范。 第四十二条:商用密码应用安全性评估、关键信息基础设施安全检测评估、网络安全等级测评应当加强衔接,避免重复评估、测评。
公安部会同相关部门	2018年6月27日	《网络安全等级保护条例(征求意见稿)》	第四十七条:非涉密网络应当按照国家密码管理法律法规和标准的要求,使用密码技术、产品和服务。第三级以上网络应当采用密码保护,并使用国家密码管理部门认可的密码技术、产品和服务。 第三级以上网络运营者应在网络规划、建设和运行阶段,按照密码应用安全性评估管理办法和相关标准,委托密码应用安全性测评机构开展密码应用安全性评估。网络通过评估后,方可上线运行,并在投入运行后,每年至少组织一次评估。密码应用安全性评估结果应当报受理备案的公安机关和所在地设区市的密码管理部门备案。
国务院第133次常务会议通过	2021年9月1日	《关键信息基础设施安全保护条例》	第五十条:存储、处理涉及国家秘密信息的关键信息基础设施的安全保护,还应当遵守保密法律、行政法规的规定。 关键信息基础设施中的密码使用和管理,还应当遵守相关法律、行政法规的规定。
国家网信办会同相关部门	2021年11月14日	《网络数据安全条例(征求意见稿)》	第九条:数据处理者应当采取备份、加密、访问控制等必要措施,保障数据免遭泄露、窃取、篡改、毁损、丢失、非法使用,应对数据安全事件,防范针对和利用数据的违法犯罪活动,维护数据的完整性、保密性、可用性。 数据处理者应当使用密码对重要数据和核心数据进行保护。



1.2 国家层面密码应用及密评相关政策文件

发文 / 起草单位	发文时间	政策文件	相关内容
国务院	2022 年 6 月 8 日	《国务院关于加强数字政府建设的指导意见》（国发〔2022〕14 号）	第三章“构建数字政府全方位安全保障体系”第二节“落实安全制度要求”中提出：加强关键信息基础设施安全保护和网络安全等级保护，建立健全网络安全、保密监测预警和密码应用安全性评估的机制，定期开展网络安全、保密和密码应用检查，提升数字政府领域关键信息基础设施保护水平。
国务院办公厅	2022 年 1 月 20 日	《国务院办公厅关于加快推进电子证照扩大应用领域和全国互通互认的意见》（国办发〔2022〕3 号）	第四章“全面提升电子证照应用支撑能力”第十四条“加强电子证照应用安全管理和监管”中提出：加强电子证照签发、归集、存储、使用等各环节安全管理，严格落实网络安全等级保护制度等要求，强化密码应用安全性评估，探索运用区块链、新兴密码技术、隐私计算等手段提升电子证照安全防护、追踪溯源和精准授权等能力。
国务院	2021 年 12 月 12 日	《“十四五”数字经济发展规划》（国发〔2021〕29 号）	第九章“着力强化数字经济安全体系”第一节“增强网络安全防护能力”中提出：提升网络安全应急处置能力，加强电信、金融、能源、交通运输、水利等重要行业领域关键信息基础设施网络安全防护能力，支持开展常态化安全风险评估，加强网络安全等级保护和密码应用安全性评估。
国务院办公厅	2019 年 12 月 30 日	《国家政务信息化项目建设管理办法》（国办发〔2019〕57 号）	第三章“建设和资金管理”第十五条、第十六条中提出：项目建设单位应当落实国家密码管理有关法律法规和标准规范的要求，同步规划、同步建设、同步运行密码保障系统并定期进行评估。 项目软硬件产品的安全可靠情况，项目密码应用和安全审查情况，以及硬件设备和新建数据中心能源利用效率情况是项目验收的重要内容。
国务院	2019 年 4 月 26 日	《国务院关于在线政务服务的若干规定》（国务院令 第 716 号）	第十三条提出：电子签名、电子印章、电子证照以及政务服务数据安全涉及电子认证、密码应用的，按照法律、行政法规和国家有关规定执行。
中共中央办公厅、国务院办公厅	2018 年 7 月 15 日	密码应用与创新发展相关工作规划	全面提升密码基础支撑能力，完善密码应用安全性评估审查机制。
国务院办公厅	2017 年 5 月 15 日	《政府网站发展指引》（国办发〔2017〕47 号）	第七章“安全防护”第一小节“技术防护”中提出：对重要数据、敏感数据进行分类管理，做好加密存储和传输。加强后台发布终端的安全管理，定期开展安全检查，防止终端成为后台管理系统的风险入口。使用符合国家密码管理政策和标准规范的密码算法和产品，逐步建立基于密码的网络信任、安全支撑和运行监管机制。

1.3 各部门密码应用及密评相关政策文件

发文 / 起草单位	发文时间	政策文件	相关内容
国家铁路局	2023 年 7 月 18 日	《铁路关键信息基础设施安全保护管理办法（征求意见稿）》	第十七条 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铁路关键信息基础设施，运营者应当使用商用密码进行保护，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。 商用密码应用安全性评估应当与铁路关键信息基础设施安全检测和风险评估、网络安全等级测评制度相衔接，避免重复评估、测评。
国家密码管理局	2023 年 6 月 9 日	《商用密码检测机构管理办法（征求意见稿）》	第三条 从事商用密码产品检测、网络与信息系统商用密码应用安全性评估等商用密码检测活动，向社会出具具有证明作用的数据、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。
国家密码管理局	2023 年 6 月 9 日	《商用密码应用安全性评估管理办法（征求意见稿）》	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。
交通运输部	2023 年 4 月 24 日	《公路水路关键信息基础设施安全保护管理办法》	第十八条 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公路水路关键信息基础设施，其运营者应当使用商用密码进行保护，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。 商用密码应用安全性评估应当与公路水路关键信息基础设施安全检测评估、网络安全等级测评制度相衔接，避免重复评估、测评。
国家密码管理局	2022 年 12 月 1 日	《关于进一步规范商用密码应用安全性评估试点工作的通知》（国密局字〔2022〕454 号）	进一步加强对密评试点工作的督促指导，强调重要网络与系统运营者密评主体责任，规范密评试点机构的日常监督，严格密评结果备案材料的形式审查，包括对密评活动真实客观性、密评实施规范有效性、密评记录清晰准确性、密评报告完整合规性等进行形式审查，并明确了对密评机构、各级密码管理部门违规行为的惩罚措施。
国家能源局	2022 年 11 月 16 日	《关于印发〈电力行业网络安全管理办法〉的通知》（国能发安全规〔2022〕100 号）	第三章“电力企业责任义务”第十五条中提出：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、关键信息基础设施网络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整改。
国家卫生健康委、国家中医药局、国家疾控局	2022 年 8 月 8 日	《医疗卫生机构网络安全管理办法》（国卫规划发〔2022〕29 号）	第二章“网络安全管理”第十五条中提出：各医疗卫生机构应依照《密码法》等有关法律法规和密码应用相关标准规范，在网络建设过程中同步规划、同步建设、同步运行密码保护措施，使用符合相关要求的密码产品和服务。



发文 / 起草单位	发文时间	政策文件	相关内容
国家邮政局、 国家发展改革委、 交通运输部	2021 年 12 月 28 日	《“十四五” 邮政业发展规 划》	第二章“主要任务”第六条“提高行业安全水平”中第十九点提出：加强网络数据安全。严格落实网络安全工作责任制，完善行业网络安全、数据安全有关标准规范。在网络建设和运营过程中，同步规划、建设、使用有关安全保护措施，严格落实国家关于等保、关保、密评等有关要求。加强行业关键信息基础设施保护，组织编制相关规划，强化行业指导和监督。加强行业重要数据和个人信息保护。
民政部	2021 年 12 月 23 日	《关于印发 “十四五” 民政信息化发 展规划的通知》 (民发〔2021〕 104 号)	第三章“重点任务”第四条中提出：全面开展国产商用密码应用，构建民政统一的密码应用基础服务平台，提供统一的数据传输、存储加密和身份认证管理等相关服务，提升密码使用和管理水平。
国家密码管理 局	2021 年 11 月 26 日	《关于规范商 用密码应用 安全性评估结 果备案工作的 通知》(国密 局字〔2021〕 392 号)	网络与信息系统运营者同步规划、同步建设、同步运行商用密码保障系统，规范开展密评工作，履行备案程序。密码管理机构对密评机构的备案材料进行形式审查，定期收集汇总备案信息，按季度报送国家密码管理局。密评机构按年度统计密评工作情况报送国家密码管理局。
国家密码管理 局、中央网信 办、国家发展 改革委、科技 部、工业和信 息化部、公安 部、财政部、 国务院国资 委、市场监 管总局、证 监会	2021 年 11 月 20 日	促进商用密码 产业高质量发 展相关文件	依法督促建设密码保障体系，并强化重要网络与信息系统商用密码应用安全性评估的执法检查。
工业和信息 化部	2021 年 9 月 15 日	《关于加强车 联网网络安全 和数据安全工 作的通知》(工 信部网安〔 2021〕134 号)	第四章“加强车联网服务平台安全防护”第十条中提出：认定为关键信息基础设施的，要落实《关键信息基础设施安全保护条例》有关规定，并按照国家有关标准使用商用密码进行保护，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。
工业和信息 化部、中央网 信办、科技部、 生态环境部、 住房城乡建设 部、农业农村 部、国家卫生 健康委、国家 能源局	2021 年 9 月 10 日	《物联网新型 基础设施建设 三年行动计划 (2021-2023 年)》(工 信部联科〔 2021〕130 号)	第二章“重点任务”第四条“支撑体系优化行动”中第十二点提出：加快物联网领域商用密码技术和产品的应用推广，建设面向物联网领域的密码应用检测平台，提升物联网领域商用密码安全性和应用水平。

发文 / 起草单位	发文时间	政策文件	相关内容
工业和信息化部、中央网信办、国家发展改革委、教育部、财政部、住房和城乡建设部、文化和旅游部、国家卫生健康委、国务院国资委、国家能源局	2021 年 7 月 5 日	《5G 应用“扬帆”行动计划（2021-2023 年）》（工信部联通信〔2021〕77 号）	第四章“提升 5G 应用支撑能力”第三条“5G 应用安全提升行动”中第三十点提出：在 5G 应用中推广使用商用密码，做好密码应用安全性评估。
交通运输部办公厅	2021 年 5 月 27 日	《关于印发〈城市轨道交通自动售检票系统运营技术规范（试行）〉的通知》（交办运〔2022〕27 号）	第九章“互联网票务”第 9.3 条“运营安全”中第 9.3.3 点提出：互联网票务的密钥使用和管理应符合国家网络安全及商用密码管理的相关法律法规，并保证支付安全。
住房城乡建设部、中央网信办、教育部、科技部、工业和信息化部、公安部、民政部、人力资源社会保障部、交通运输部、商务部、文化和旅游部、国家卫生健康委、应急部、市场监管总局、广电总局、体育总局	2021 年 4 月 6 日	《关于加快发展数字家庭提高居住品质的指导意见》（建标〔2021〕28 号）	第四章“完善数字家庭系统”第四条中提出：强化网络和数字安全保障。数字家庭系统应同步规划、同步建设、同步使用网络安全技术。按照法律法规规定和国家强制性标准要求，采取技术等必要措施，保障数字家庭系统安全稳定运行，防止信息泄露、损毁、丢失，确保收集、产生数据和个人信息安全。遵守密码应用规定，形成安全可控完整的产业生态系统。
国家卫生健康委办公厅、国家中医药局办公室	2020 年 9 月 27 日	《关于加强全民健康信息标准化体系建设的意见》（国卫办规划发〔2020〕14 号）	第二章“全民健康信息标准化体系建设的重点任务”第四条“加强网络安全标准化建设”中第一点提出：完善行业网络安全标准体系。贯彻《中华人民共和国网络安全法》，推进网络安全等级保护、商用密码应用、关键信息基础设施保护等制度在行业落地实施，研究编制卫生健康行业网络安全技术、医疗卫生机构安全能力评估、关键信息基础设施识别认定和保护等标准。



发文 / 起草单位	发文时间	政策文件	相关内容
公安部	2020 年 7 月 22 日	《贯彻落实网络安全等级保护制度和关键信息基础设施安全保护制度的指导意见》（公网安〔2020〕1960号）	第二章“深入贯彻实施国家网络安全等级保护制度”第六条中提出：落实密码安全防护要求。网络运营者应贯彻落实《密码法》等有关法律法规规定和密码应用相关标准规范。第三级以上网络应正确、有效采用密码技术进行保护，并使用符合相关要求的密码产品和服务。第三级以上网络运营者应在网络规划、建设和运行阶段，按照密码应用安全性评估管理办法和相关标准，在网络安全等级测评中同步开展密码应用安全性评估。
国家发展改革委办公厅	2020 年 7 月 9 日	《关于加快落实新型城镇化建设补短板强弱项工作有序推进县城智慧化改造的通知》（发改办高技〔2020〕530号）	第三章“重点方向”第四条中提出：健全网络安全防护体系，做好网络安全与智慧化改造一体化推进。落实网络安全工作责任制要求，完善智慧化改造网络安全管理制度规范。认真落实国家网络安全等级保护、网络安全审查、云计算采购服务、国家密码管理等有关规定，采购部署安全可靠的软硬件产品，具备与智慧化水平相匹配的体系化安全防护能力。
教育部办公厅	2020 年 2 月 26 日	《2020 年教育信息化和网络安全工作要点》（教科技厅〔2020〕1号）	第三章“重点任务”第五条“全面推进教育治理能力优化行动”中第十五点提出：加强教育系统密码应用与管理。落实《教育行业密码与应用创新发展实施方案》，推进密码基础设施和支撑体系建设，有序推动教育重要业务信息系统开展密码应用安全性评估，完善教育数字认证（CA）基础支撑体系建设，推动国家教育管理信息系统密码普遍应用，提升系统安全和数据安全。
水利部办公厅	2020 年 2 月 14 日	《2020 年水利网信工作要点》（办信息〔2020〕22号）	第一章“补水利网信短板”第一条“补水利网络安全短板”中第二点提出：推进商用密码应用。组织宣贯《中华人民共和国密码法》，开展水利行业密码应用专题调研，出台推进商用密码应用具体措施。落实《水利部密码应用与创新发展实施方案（2018-2022年）》，持续推进三峡水利枢纽、南水北调工程等重要水利基础设施和国家水资源管理系统等重要信息系统的密码应用。
交通运输部	2019 年 12 月 9 日	《关于印发〈推进综合交通运输大数据发展行动纲要（2020-2025年）〉的通知》（交科技发〔2019〕161号）	第三章“主要任务”第四条“加强大数据安全保障”中第十八点提出：完善数据安全保障措施。推进交通运输领域数据分类分级管理，加强重要数据和个人信息安全保护，制定数据分级安全管理、数据脱敏等制度规范。推进重要信息系统密码技术应用和重要软硬件设备自主可控。
国家能源局	2018 年 9 月 13 日	《国家能源局关于加强电力行业网络安全工作的指导意见》（国能发安全〔2018〕72号）	第五章“加强行业网络安全基础设施建设”第十四条中提出：加快密码基础设施建设。在重要业务、重要领域实施密码保护，完善电力行业密码支撑体系，实现电力行业密码基础设施一体化管理。健全电力行业密码检测手段，开展密码应用安全性评估。深化商用密码在电力行业中的应用，促进密码技术与电力应用融合发展。

发文 / 起草单位	发文时间	政策文件	相关内容
交通运输部办公厅	2018 年 1 月 31 日	《交通一卡通运营服务质量管理办法（试行）》（交办运〔2018〕17 号）	第八章“安全管理”第六十一条中提出：交通一卡通运营机构应当按照国家关于网络安全及商用密码管理的法律和行政法规相关规定，使用交通一卡通商用密码，推动国产商用密码应用，落实业务数据和信息的安全保护责任，保障交通一卡通信息安全。
财政部	2017 年 12 月 26 日	《政务信息系统政府采购管理暂行办法》（财库〔2017〕210 号）	第八条提出：采购需求应当落实国家密码管理有关法律法规、政策和标准规范的要求，同步规划、同步建设、同步运行密码保障系统并定期进行评估。 第十二条提出：采购人应当按照国家有关规定组织政务信息系统项目验收，根据项目特点制定完整的项目验收方案。验收方案应当包括项目所有功能的实现情况、密码应用和安全审查情况、信息系统共享情况、维保服务等采购文件和采购合同规定的内容，必要时可以邀请行业专家、第三方机构或相关主管部门参与验收。

1.4 各省（自治区、直辖市）及新疆生产建设兵团密码应用及密评相关政策文件

省（自治区、直辖市）、新疆生产建设兵团	发布时间	政策文件	相关内容
北京市	2021 年 5 月	《政府投资信息化项目密码应用工作规范》	新建网络和信息系统应当采用国产密码进行保护，同步规划、同步建设、同步运行密码保障系统，定期开展密码应用安全性评估，已建网络和信息系统应当进行密码国产化改造，确保使用的密码算法和技术符合国家的法律法规和相关标准，使用的密码产品和服务通过国家密码管理部门的核准或许可。
	2019 年 4 月	《关于在政府投资信息化项目建设中规范使用密码的通知》	项目实施单位要同步规划、同步建设、同步运行密码保障系统，定期开展密码应用安全性评估，确保不新增安全风险。
天津市	2021 年 12 月	《天津市政务信息化项目建设管理办法》	市级政务信息化项目建设应当符合国家和天津市网络安全、数据安全、密码使用相关要求；项目建设部门应当落实国家密码管理有关法律法规和标准规范的要求，同步规划、同步建设、同步运行密码保障系统并定期进行密码应用安全性评估。
	2020 年 7 月	《关于切实做好政务信息化项目密码应用工作的通知》	政务信息化项目建设单位，在申请项目资金前应当按通知要求向密码管理部门提交材料，进行密码使用合规性审核；在完成项目建设任务后，进行密评；在项目验收运行后，定期开展密评。



省(自治区、直辖市)、新疆生产建设兵团	发布时间	政策文件	相关内容
河北省	2020 年 11 月	《关于进一步加强非涉密政务信息系统密码应用与安全性评估工作的通知》(冀国密局字〔2020〕12 号)	落实《河北省省级政务信息化项目建设管理办法》(冀政办字〔2020〕48 号)要求,规范省内非涉密政务信息系统立项、实施、验收阶段密码保障系统建设、管理,落实“三同步一评估”要求。
	2020 年 4 月	《河北省省级政务信息化项目建设管理办法》(冀政办字〔2020〕48 号)	第十九条提出:项目建设单位应当落实国家密码管理有关法律、法规和标准规范的要求,同步规划、同步建设、同步运行密码保障系统并定期进行评估。 第三十七条提出:省各部门应当严格遵守有关保密等法律、法规规定,构建全方位、多层次、一致性的防护体系,按要求采用密码技术,并定期开展密码应用安全性评估,确保政务信息系统运行安全和政务信息资源共享交换的数据安全。
	2019 年 3 月	《关于开展重要信息系统密码应用安全性评估的通知》(冀国密局字〔2019〕2 号)	贯彻落实中央文件精神,组织省内有关单位对其建设使用的重要信息系统开展密评,省密码管理部门对工作情况和评估发现问题开展监督检查。
山西省	2022 年 10 月	《山西省财政厅关于在政府采购中落实密码应用的通知》(晋财〔2022〕13 号)	各预算单位要严格按照《密码法》及相关要求推进密码应用,涉及金融及重要领域的信息化项目要同步规划、同步建设、同步运行密码保障系统,保障网络和信息安全。
	2021 年 8 月	《山西省政务云管理办法》(晋政办发〔2021〕72 号)	第五章“安全管理”第二十四条中提出:政务云服务提供方和政务云使用部门要严格落实密码应用法律法规和相关政策,使用符合国家技术标准规范的软硬件产品及密码,优先使用自主可控的软硬件产品,定期开展密码应用安全性评估。
	2019 年 9 月	《山西省政务信息化项目建设应用管理办法》(晋政办发〔2019〕72 号)	第五章“管理和安全”第三十七条中提出:项目实施单位与项目建设单位共同开展网络与信息安全风险评估,严格落实等级保护和国家密码管理要求,同步规划、同步建设、同步运行密码保障系统并定期评估,切实保障政务信息系统安全稳定运行。
内蒙古自治区	2023 年 1 月	《内蒙古自治区“十四五”期间商用密码重点工作任务》(内国密局发〔2023〕1 号)	加强商用密码应用安全性评估和管理。推动关键信息基础设施、等级保护三级及以上信息系统、全区政务信息系统等同步规划、同步建设、同步运行密码保障系统,定期开展商用密码应用安全性评估;加强与政务信息化项目审批部门的工作协同,严格落实商用密码应用闭环管理要求;加强对密评机构的指导和管理,探索建立用户评价机制,持续提升密评机构能力水平;根据国家总体部署,按照科学布局、强优兼顾、考核认定的原则,适时培育商用密码应用安全性测评机构;持续优化“内蒙古自治区商用密码业务监管平台”功能,推进商用密码应用动态监测,加强商用密码应用信息归集管理,适时与国家平台对接。

省(自治区、直辖市)、新疆生产建设兵团	发布时间	政策文件	相关内容
内蒙古自治区	2022 年 12 月	《自治区本级政务信息化项目建设暂行管理办法》(内发改高技字〔2022〕1963 号)	第十二条第二点提出:备案文件应当包括项目名称、……、密码应用方案和密码应用安全性评估报告等内容。 第三十四条提出:各项目单位和建设(代建)单位应当严格遵守有关保密等法律法规规定,构建全方位、多层次、一致性的防护体系,按要求采用密码技术,并定期开展密码应用安全性评估和等保测评,确保政务信息系统运行安全和政务信息资源共享交换的数据安全。
	2022 年 11 月	《内蒙古自治区数字经济促进条例(草案)》	第七章“安全保障”第六十五条中提出:网络运营者应当依法进行安全评估,采取软件测评、风险评估、安全漏洞分析和预警监测、网络安全等级保护、商用密码应用安全性评估、数据安全测评等安全技术措施,保障数据、网络、设施等方面的安全。
	2022 年 1 月	《关于规范全区商用密码应用安全性评估结果备案工作的通知》(内国密局发〔2022〕1 号)	本地区、本部门(行业)的网络与信息系统运营者为备案主体。网络与信息系统运营者应按照国家、自治区有关规定,同步规划、同步建设、同步运行商用密码保障系统,规范开展密评工作,履行备案程序。
	2021 年 11 月	《关于做好自治区本级政务信息化项目商用密码应用安全性评估工作的通知》(内国密局发〔2021〕7 号)	一、本级新建政务信息化项目要认真落实国家密码管理应用有关法律法规和标准规范要求,同步规划、同步建设、同步运行密码保障系统并定期进行评估。 二、本级新建政务信息化项目在编制项目建议书、可行性研究报告和初步设计时,要单设章节专题阐述密码建设内容并编制密码应用方案。项目报竣申请验收时,要提供密码测评报告,报告结论未通过的,不得提请验收。
	2021 年 9 月	《内蒙古自治区商用密码事中事后监管方案》(内国密局发〔2021〕5 号)	1. 监管事项(1)非涉密关键信息基础设施、网络安全等级保护第三级及以上信息系统、国家政务信息系统等重要网络和 Information 系统中商用密码应用的合规性、正确性、有效性; 4. 监管方式和检查频次、监管方式:现场检查和委托第三方检测机构检测相结合。检查频次:从非涉密关键信息基础设施、网络安全等级保护第三级及以上信息系统、国家政务信息系统等重要网络和 Information 系统中随机抽取,随机检查比例为每年 10%-20%。3 年内已被随机检查、无违规行为的,不列入随机检查范围。对随机检查不合格的部门单位加大检查频次。
辽宁省	2021 年 6 月	《辽宁省省级政务信息化建设项目预算申报指南》(辽财办函〔2021〕382 号)	第三章“申报内容”第七节“工程建设其他经费”中提出:工程建设其他经费是项目单位根据相关文件规定和要求,结合项目类型和规模等因素,聘请相应的第三方服务机构提供相应服务所产生的费用,包括项目咨询(设计)服务费、工程监理费、网络安全等级保护测评费、第三方测试费、密码应用安全性评估费等内容。



省(自治区、直辖市)、新疆生产建设兵团	发布时间	政策文件	相关内容
辽宁省	2020 年 10 月	《关于进一步加强政务信息化系统密码应用与安全性评估工作的通知》(辽密局发〔2020〕26 号)	该文件对辽宁省内非涉密政务信息系统立项、建设、验收等过程中使用密码和开展密评工作提出要求。
吉林省	2022 年 5 月	《吉林省促进商用密码产业高质量发展行动计划》(吉密局发〔2022〕1 号)	该计划提出:依法督促我省重要网络和信息系统运营者同步规划、同步建设、同步运行密码保障系统,定期开展商用密码应用安全性评估;加强关键信息基础设施安全保护制度、网络安全等级保护制度与商用密码应用安全性评估要求的衔接;规范数据分类分级保护、互联网平台和个人信息处理者的密码使用管理。
	2021 年 12 月	《关于落实商用密码应用安全性评估结果备案工作的通知》(吉密协办〔2021〕21 号)	各地区、省直各部门网络与信息系统运营者按照法律、法规、规章和国家有关规定,同步规划、同步建设、同步运行商用密码保障系统,规范开展密评工作。 严格履行备案程序,各地区、省直各部门网络与信息系统运营者自密评报告出具之日起 30 日内,填写《网络与信息系统密评备案信息表》,连同密评报告报省密码管理局备案。 各地区密码管理部门负责指导、汇总报送本地区网络与信息系统备案工作。
	2021 年 6 月	《吉林省数字政府建设“十四五”规划》(吉政数综合〔2021〕8 号)	第十一章“建设安全可靠的管理运维体系”第一节“建立安全管理和运维工作机制”中提出:严格落实网络安全法律法规和政策标准要求,推动安全可靠技术和产品在重要领域的应用,推动政务云平台获得安全认证,政务信息系统落实信息系统安全等级保护、风险评估、商密评估等有关要求。推动自主可控信息化产品和国产密码在相关领域的应用,提升密码基础支撑能力,确保数字政府建设自主可控、安全高效运行。
	2020 年 10 月	《关于进一步做好政务信息化系统密码应用与安全性评估工作的通知》(吉密协办〔2020〕16 号)	政务信息系统规划、建设、运行阶段,项目建设单位要严格落实国家密码管理有关规定和规范要求,同步规划、同步建设、同步运行密码保障系统,并定期进行评估。 委托开展商用密码应用安全性评估的,应从《商用密码应用安全性评估试点机构目录》中选择评估机构。 商用密码应用安全性评估工作相关材料需报省密码管理局备案。
	2020 年 9 月	吉林省政务信息化项目建设管理办法(吉政数联〔2020〕9 号)	第一章“总则”第五条中提出:省密码管理局负责政务信息化系统密码应用的指导、监督和检查工作。指导项目建设单位按要求采用密码技术、密码产品、密码服务,并定期开展密码应用安全性评估,确保政务信息系统运行安全和政务信息资源共享交换的数据安全。

省(自治区、直辖市)、新疆生产建设兵团	发布时间	政策文件	相关内容
黑龙江省	2022年3月	《关于规范商用密码应用安全性评估结果备案工作的通知》	旨在规范和强化黑龙江省密评备案程序,要求网络与信息系统运营者,应同步规划、同步建设、同步运行商用密码保障系统,自行或者委托商用密码检测机构开展密评工作,履行备案程序。自密评报告出具之日起30日内,填写《网络与信息系统密评备案信息表》,连同密评报告报同级密码管理部门备案。
	2021年12月	《黑龙江省“十四五”数字政府建设规划》(黑政发〔2021〕17号)	第四章“夯实四大数字基础支撑底座”第四节“构建全省一体化安全防护体系”第一条“提升安全保障能力”中提出:完善密码基础设施建设,建立信任服务体系,为资源安全利用和行为可信提供支撑。强化安全防护技术支撑能力。加强数字政府密码应用服务能力,同步规划、同步建设、同步运行密码保障系统,推进政务信息化系统密码改造工作,并定期进行评估。
	2021年4月	《黑龙江省省级政务云管理暂行办法》(黑政办发〔2021〕17号)	第一章“总则”第六条中提出:省政务云按照国家密码管理有关法律法规和标准规范要求,同步规划、同步建设、同步运行密码保障系统。
	2020年11月	《关于进一步加强政务信息系统密码应用与安全性评估工作的通知》	旨在推动和加强黑龙江省政务信息系统密码应用与安全性评估工作,要求我省非涉密政务信息系统项目建设单位同步规划、同步建设、同步运行密码保障系统并定期进行密码应用安全性评估,保障密码应用与安全性评估经费,配备密码保障系统管理和运维人员。
上海市	2022年8月	《上海市市级数字化项目支出预算管理暂行办法》(沪经信推〔2022〕535号)	明确将密码产品、密码服务列入建设类、运维类项目的支出范围。申报数字化项目应当严格落实密码应用要求。将密码应用情况作为建设类项目评审重点之一。项目实施时需落实密码应用要求。项目验收时需提交密码应用测评报告。
	2022年5月	《上海市重要网络和信息系统密码应用与安全性评估工作指南(2022版)》	第二章“密码应用与安全性评估范围”中提出:对于涉及国家安全和社会公共利益的重要网络和信息系统,包括非涉密的关键信息基础设施、网络安全等级保护第三级以上网络(含信息系统)、政务信息系统,以及法律、行政法规和国家有关规定要求使用商用密码进行保护的其他网络和信息系统,应当落实密码有关法律法规、管理办法和标准规范的要求,同步规划、同步建设、同步运行密码保障系统并定期进行评估。
	2022年4月	《上海市政务云管理暂行办法》(沪府办规〔2022〕6号)	政务云服务商负责建立健全安全保护工作制度,提供安全可信的产品和服务,做好政务云的安全监测和防御工作,定期开展网络安全等级保护测评与密码应用安全性评估,保障政务云安全稳定运行。 政务云主管部门、政务云运行管理单位和使用单位应当严格落实国家网络安全和商用密码应用要求,采取安全措施,并与政务云同步规划、同步建设、同步运行网络安全体系与密码保障体系。



省(自治区、直辖市)、新疆生产建设兵团	发布时间	政策文件	相关内容
上海市	2022 年 4 月	《上海市电子政务云政务移动办公信息系统密码应用建设指南(暂行)》	可用于指导政务移动办公信息系统的责任单位规范开展密码应用与安全性评估工作,也可供系统集成单位、密码应用支撑单位和商用密码检测机构参考。各级地方政务移动办公信息化建设、使用、管理单位也可参照《指南》开展相关工作。
	2022 年 2 月	《关于进一步加强我市电子政务云及上云信息系统密码应用工作的通知》	加强上海市电子政务云及上云信息系统密码应用与安全性评估工作。
	2021 年 5 月	《关于规范和加强我市重要网络和信息系统密码应用与安全性评估工作的通知(含上海市重要网络和信息系统密码应用与安全性评估工作指南(2021 版))》	明确密码应用与安全性评估的范围、要求、工作实施流程和保障措施,规范和加强上海市重要网络和信息系统密码应用与安全性评估工作。
	2020 年 3 月	《关于进一步加强和规范关键信息基础设施密码应用工作的通知》	规范和加强上海市关键信息基础设施密码应用与安全性评估工作。
江苏省	2022 年 4 月	《省政府关于加快统筹推进数字政府高质量建设的实施意见》(苏政发〔2022〕44 号)	第五章“织密筑牢网络数据安全防火墙”第十六条“严格执行安全管理制度”中提出:依法加强数据安全防护,落实网络安全等级保护、关键信息基础设施安全保护、数据分类分级保护、密码应用管理等制度。
	2022 年 3 月	《关于规范密码应用安全性评估结果备案工作的通知》(苏密局字〔2022〕7 号)	进一步规范省各有关部门、单位的密评与备案工作,明确密评和备案工作情况将作为网络安全工作责任制落实情况有关密码管理考核依据。
	2021 年 4 月	《江苏省省级政务信息化项目建设管理办法》(苏政办发〔2021〕24 号)	第三章“建设和资金管理”第十八条中提出:项目建设单位应当落实国家和省密码管理有关法律法规和标准规范的要求,同步规划、同步建设、同步运行密码保障系统并定期进行评估。
	2020 年 8 月	《江苏省政务信息化项目密码应用与评估备案指南(试行)》(苏密局字〔2020〕43 号)	该文件提出政务信息化项目密码应用与评估备案工作的要求和具体流程。

省(自治区、直辖市)、新疆生产建设兵团	发布时间	政策文件	相关内容
浙江省	2022 年 9 月	《关于对密评结果开展审查工作的通知》	对自 2022 年 1 月起至 2022 年 12 月底之前全省开展的密评项目，重点对各地各单位新建等保三级以上政务信息系统，《浙江省密码应用与创新发展实施方案》涉及的重要网络与信息系统的密评结果，逐项核查密评活动是否客观、密评实施是否规范有效、密评记录是否清晰准确等。
	2022 年 8 月	《电子政务建设项目申报工作的通知》	建设项目应按照国家有关规定和标准明确网络安全保护等级或密级，设计和采取网络安全保护措施。非涉密项目方案应包括符合国家标准设计的密码应用设计方案，重要网络与信息系统项目应按要求规划商用密码应用安全性评估。新建项目网络安全预算不低于项目总投资 5%。
	2022 年 7 月	《浙江省人民政府关于深化数字政府建设的实施意见》（浙政发〔2022〕20 号）	第五章“构建数字政府全方位安全保障体系”第二条“落实安全制度要求”中提出：严格落实相关法律法规制度，全面贯彻《浙江省公共数据条例》，健全数据归集、治理、共享、开放、授权运营、安全管理等制度。建立网络安全等级保护、涉密信息系统分级保护、密码应用安全性评估制度，完善网络安全标准规范。探索建立首席网络安全官制度。
	2022 年 3 月	《关于深入开展密码应用安全性评估工作的通知》	2022 年，各地各单位新建等保三级及以上政务信息系统，必须落实商用密码应用安全性评估要求：同步规划、同步建设、同步运行商用密码保障系统，选择经国家密码管理局认可、具备相关资质的检测机构开展密码应用安全性评估工作，并基本符合密码应用要求。
	2022 年 1 月	《浙江省电子政务外网安全评估指标体系（试行）》	安全防护层面中要求：统一建设密码服务平台，为本地区提供密码服务；对本地区网络安全等保三级及以上政务信息系统开展商用密码应用安全性评估。
	2021 年 12 月	《关于规范商用密码应用安全性评估结果备案工作的通知》（浙密局发〔2021〕29 号）	请各地市各部门指导督促本地区、本部门（行业）有关网络与信息系统运营者自密评报告出具之日起 30 日内，填写备案信息表并在规定期限内将表格与密评报告报省密码局备案；请各市密码管理部门定期收集汇总所在地区的密评结果备案信息，填写《密评备案信息汇总表》按季度报送省密码管理局。
	2021 年 10 月	《关于加强浙江辖区证券期货业密码应用工作的通知》（浙证监机构字〔2021〕120 号）	辖区各经营机构应当于 2021 年底前，完成方案制定和评审。2022 年 12 月前，完成系统改造、安全性评估及收尾工作；辖区国有控股证券公司、期货公司、基金管理公司、独立基金销售机构应严格按照要求开展密码应用工作，鼓励民营和外资机构资源开展相关工作；辖区各经营机构应当积极参与证券业协会、期货业协会、基金业协会组织开展的密码应用专项培训。



省(自治区、直辖市)、新疆生产建设兵团	发布时间	政策文件	相关内容
安徽省	2023 年 1 月	《数字安徽建设 2023 年重点工作安排》	加强对基础网络、数据中心、工业互联网平台等关键信息基础设施的安全防护，定期开展网络安全等级保护和商用密码应用安全性评估。
	2022 年 10 月	《安徽省政务信息化项目建设管理办法》（皖数安〔2022〕2 号）	第四章“项目建设管理”第三十条中提出：项目建设单位应当按照国家密码管理有关法律法规和标准规范要求，同步规划、同步建设、同步运行密码保障系统并定期进行密码应用安全性评估。
	2022 年度	《综合绩效考核依据》	根据《安徽省金融和重要领域密码应用于创新发展实施方案（2019-2022 年）的通知》，本部门新建、改建、扩建（含规划和建设中）的非涉密信息系统无密码应用且未作出相应规划安排的扣 0.5 分。
	2021 年 12 月	《关于规范商用密码应用安全性评估结果备案工作的通知》	项目建设单位应落实国家密码管理有关法律法规和标准规范的要求，使用商用密码进行保护，同步规划、同步建设、同步运行密码保障系统并定期开展密码应用安全性评估。
福建省	2022 年 12 月	《福建省数字政府改革和建设总体方案》（闽政〔2022〕32 号）	全面推进重要领域商用密码应用，落实国家密码管理有关法律法规和标准规范的要求，同步规划、同步建设、同步运行商用密码保障系统并定期进行商用密码应用安全性评估。
	2022 年 3 月	《关于加强商用密码应用与安全性评估工作的通知》（闽密〔2022〕1 号）	网络与信息系统建设单位应当同步规划、同步建设、同步运行商用密码保障系统并定期进行商用密码应用安全性评估。
	2021 年 11 月	《福建省“十四五”数字福建专项规划》（闽政〔2021〕25 号）	第八章“筑牢可信可靠的网络安全屏障”第二节“完善网络安全监管体系”中提出：全面落实网络安全等级保护国家标准，坚持“自主可控”原则，完善密码基础设施建设，健全密码应用安全评估机制。
	2017 年 11 月	《关于在数字福建建设项目可研暨初设编写提纲增加重要领域密码应用章节的通知》（闽数字办〔2017〕14 号）	增加重要领域密码应用独立章节，要求安全系统设计根据系统安全等级保护级别，按照《信息系统密码应用基本要求》进行设计。
江西省	2021 年 8 月	《江西省电子印章管理暂行办法》（赣府厅字〔2021〕61 号）	第六章“安全管理”第二十七条中提出：具备完善的信息安全防护措施，通过商用密码应用安全性评估，至少符合信息系统安全保护等级三级要求。
	2020 年 9 月	《江西省政务信息化项目建设管理办法》（赣府厅字〔2020〕68 号）	第三章“建设和资金管理”第十五条中提出：项目建设单位应当按照《中华人民共和国网络安全法》《中华人民共和国密码法》等法律法规以及党政机关安全管理等有关规定，建立网络安全和密码安全等管理制度，同步规划、同步建设、同步运行密码保障系统，定期开展网络安全检测与风险评估，保障信息系统安全稳定运行。

省(自治区、直辖市)、新疆生产建设兵团	发布时间	政策文件	相关内容
山东省	2022 年 1 月	《关于规范商用密码应用安全性评估结果备案工作的通知》(鲁密局字〔2022〕1 号)	该文件对各市和省有关部门、单位开展密评结果备案工作作了具体要求。
	2021 年 7 月	《山东省“十四五”数字强省建设规划》(鲁政字〔2021〕128 号)	推动密码创新和融合应用,落实密码应用与安全性评估要求,塑造政务系统密码服务保障体系。
	2021 年 1 月	《关于促进山东省网络安全产业发展的指导意见》(鲁网办发〔2021〕1 号)	第二章“主要任务”第二条“服务模式升级”中提出:推动网络安全企业由提供安全产品向提供安全服务和解决方案转变,支持专业机构和企业开展网络安全规划咨询、安全集成、风险评估、检测认证、密码服务和检测、威胁监测、应急响应、安全运维、安全培训等安全服务。
	2020 年 4 月	《山东省政务云平台管理暂行办法》(鲁数字〔2020〕7 号)	政务云节点服务商应严格落实网络安全、保密、密码等相关法律法规,建立安全管理体系,定期开展网络安全等级保护测评、……、商用密码应用安全性评估等工作。
河南省	2023 年 1 月	《河南省非涉密政务信息系统安全建设指南(试行)》(豫数政办〔2023〕1 号)	要求建设单位应根据政务信息系统安全保护等级,明确密码应用等级及需求,并编制密码应用方案;政务信息系统应于上线前和运维期间每年开展安全风险评估,安全保护等级第三级及以上系统还应同时开展密码应用安全性评估工作,并根据密评报告进行整改。 要求运维单位应根据密码管理部门的安全通报,对政务信息系统进行风险排查和安全加固。 要求建设单位应依法通过政府采购方式确定承担密码应用安全性评估的单位,并直接签订合同,严禁层层转包分包。
	2023 年 1 月	《河南省促进商用密码产业高质量发展若干政策措施》(豫发改数字〔2023〕13 号)	支持商用密码在全省非涉密政务信息系统、关键信息基础设施、网络安全等级保护第三级以上网络建设中的应用,依法督促重要网络和信息系統建设单位同步规划、同步建设、同步运行密码保障系统并定期开展商用密码应用安全性评估,落实评估结果备案制度。强化重要网络与信息系統商用密码应用与安全性评估情况的执法检查。加强电子政务电子认证密码基础设施建设,积极稳妥推动电子印章、电子证照等领域密码应用。支持重点企业开展政务、金融、交通、能源、医疗等领域密码应用示范,遴选推广典型场景优秀密码应用方案,推荐申报国家级商用密码试点示范。
	2022 年 11 月	《河南省网络安全条例》(2022 年 11 月 26 日河南省第十三届人民代表大会常务委员会第三十六次会议通过)	第十九条提出:县级以上网信、公安等有关部门应当指导督促网络运营者落实关键信息基础设施安全保护、网络安全等级保护、数据安全保护、个人信息保护、密码应用安全性评估、云计算服务安全评估、网络信息安全投诉举报等制度,落实相关国家标准的强制性要求,制定网络安全事件应急预案。



省(自治区、直辖市)、新疆生产建设兵团	发布时间	政策文件	相关内容
河南省	2022 年 10 月	《河南省加快推进电子证照等“四电”扩大应用和互通互认实施方案》(豫政办〔2022〕101 号)	提高“四电”支撑系统、应用系统安全保障能力,严格落实网络安全等级保护、商用密码应用安全性评估等要求,增强系统入侵防御、数据库审计等功能。
	2022 年 9 月	《河南省大数据产业发展行动计划(2022-2025 年)》(豫政办〔2022〕90 号)	第三章“主要任务”第七节“构建安全保障体系”中提出:实施数据安全“铸盾”行动,定期开展关键设施和系统安全检查、风险评估,建设网络安全应急体系。依法使用密码保护数据安全,定期开展密码应用安全性评估,落实网络安全等级保护和保密等要求。
	2022 年 4 月	《河南省政务数据安全暂行管理办法》(豫政办〔2022〕39 号)	第七条提出:网信部门负责统筹协调、检查指导和相关监督管理等工作。公安部门负责等级保护、日常巡查、执法检查、信息通报、应急处置等监督管理工作。保密、国家安全、密码管理、大数据管理、通信管理等部门按照本办法和有关法律、法规、规章的规定,在各自职责范围内承担政务数据安全监管职责。 第十一条提出:政务部门应落实等级保护、密码应用等要求,定期开展政务信息系统等级保护和商用密码应用等安全性评估。
	2022 年 1 月	《河南省“十四五”新型基础设施建设规划》(豫发改数字〔2022〕52 号)	“推动新型基础设施全部纳入关键信息基础设施保护范围,确保网络安全防护设施与新型基础设施同步规划、同步建设、同步使用。”“健全网络安全监测预警响应机制,构建以密码技术为核心、多种技术相互融合的网络安全保障体系,加强重要新型基础设施可靠性保障。”“推广安全可信、自主可控的网络产品和服务,强化密码技术在重要新型基础设施中的应用。”“严格落实网络安全工作责任制,严格执行网络安全等级保护、密码应用安全性评估等相关政策法规和标准规范要求”
	2021 年 12 月	《关于做好商用密码应用安全性评估结果备案工作的通知》(豫密局电〔2021〕55 号)	根据《关于规范商用密码应用安全性评估结果备案工作的通知》(国密局字〔2021〕392 号),对河南省区域内密评及备案工作进行部署安排,提出有关备案要求。
	2021 年 10 月	《关于开展我省重要领域网络和信息系统密码应用安全性评估工作的通知》(豫密局电〔2021〕40 号)	2021 年 10 月,河南省密码管理局例行开展年度密评检查,要求各单位对已建重要领域网络和信息系统开展密码应用安全性自查,并抽取部分系统进行密评。
	2020 年 11 月	《关于进一步加强政务信息系统密码应用与安全性评估工作的通知》(豫密局字〔2020〕35 号)	根据国家密码管理局《关于请进一步加强国家政务信息系统密码应用与安全性评估工作的函》(国密局函〔2020〕119 号),河南省密码管理局、发展改革委、财政厅、大数据管理局联合印发文件,就河南省非涉密政务信息系统密码应用与安全性评估工作提出“三同步一评估”、保障密码应用与安全性评估经费、配备密码保障系统管理和运维人员等要求。

省(自治区、直辖市)、新疆生产建设兵团	发布时间	政策文件	相关内容
湖北省	2022 年 12 月	《湖北省商用密码应用安全性评估工作指南(2022 版)》	为更好指导非涉密关键信息基础设施、网络安全等级保护第三级以上网络、国家政务信息系统等网络与信息系统密码应用与安全性评估工作,汇编有关法律法规与政策文件、密码应用标准规范、应用方案示例、常见问题解答,形成《湖北省商用密码应用与安全性评估工作指南(2022 版)》
	2022 年 8 月	《关于印发深化数据赋能扩大“免证明”应用领域工作方案的通知》(政办发〔2022〕42 号)	加强电子证照应用安全监管。落实国家相关法律法规要求,完善电子证照管理规章制度,加强电子证照制发、归集、存储和使用环节的信息安全管理,防范未经授权擅自调用、留存电子证照等风险。对涉及个人隐私的证照数据,严格落实持证主体认证授权机制,充分保障持证主体的知情权、决定权。各地要加强数据安全自查和监管,强化电子证照数据和应用接口的安全防护,严格遵守网络安全等级保护制度规定,强化国产密码应用和安全性评估,主动感知发现和及时处置异常调用、非法访问等情况。
	2021 年 12 月	《关于规范全省商用密码应用安全性评估结果备案工作的通知》(鄂密局发〔2021〕3 号)	各地区、各部门(行业)有关网络与信息系统运营者应按照法律、法规、规章和国家有关规定,同步规划、同步建设、同步运行密码保障系统,规范开展密评工作,履行备案程序。
	2021 年 8 月	《进一步加强政务信息系统密码应用与安全性评估工作的通知》(鄂密局发〔2021〕2 号)	新建、扩建、改建以及通过政府购买服务产生的政务信息系统,项目建设单位应当同步规划、同步建设、同步运行密码保障系统并定期评估,采用符合国家标准密码算法、技术,使用具有《商用密码产品认证证书》的密码产品和国家主管部门许可的密码服务。密码应用方案及密码应用方案评估报告是项目立项环节的必备材料,结论为“符合”或“基本符合”的密码应用安全性评估报告是项目验收环节的必备材料。未进行密码应用安全性评估或评估不合格的政务信息系统,不得继续投入运行。
	2020 年 7 月	《关于印发湖北省数字政府建设总体规划(2020-2022 年)的通知》(鄂政发〔2020〕12 号)	加快安全管理系统建设,建设省市县三级全域安全态势与预警处理、云安全能力平台、安全数据分析平台、终端安全管理系统、攻防演练平台、密码支撑体系等。强化自主可控技术支撑,根据国家法律、政策法规、文件要求采用国产密码及自主可控的技术和产品,建设数字政府国产密码基础支撑体系,开展国产密码应用安全性评估工作、建立健全密码应用及自主可控安全性评估审查制度,助推云操作系统、数据库、中间件、大数据等方面国产化替代进程,推动安全可靠技术和产品在重要领域的应用。
	2018 年 9 月	《湖北省政务信息化项目建设管理办法》(鄂政办发〔2018〕59 号)	第三章“安全管理”第十三条中提出:项目建设单位应开展网络与信息安全风险评估,严格落实等级保护、分级保护和密码管理的要求,同步规划、同步建设、同步运行密码保障系统并定期评估,切实保障政务信息化项目安全稳定运行。



省(自治区、直辖市)、新疆生产建设兵团	发布时间	政策文件	相关内容
湖北省	2015 年 12 月	《关于促进电子政务协调发展的实施意见》(鄂政办发〔2015〕95 号)	完善安全防护体系,按照密码应用规范的要求,构建全省电子政务安全防护体系。制定统一安全策略,划分安全域,保障基础信息网络、重要信息资源库、重点业务系统和安全基础设施的安全。推动信任服务体系建设,建立符合国家相关标准规范的统一认证、授权管理、可信时间等安全基础设施。加大自主可控信息安全产品运用。强化安全保密意识,加强日常安全管理,落实密码管理相关主体责任。
湖南省	2022 年 3 月	《政务信息化项目网络安全审查规范》(DB43/T 2313-2022)	第五章“审查前合规性自查”第一节“方案编制”中提出:建设单位应对项目安全需求进行分析,并根据安全需求组织编制项目安全设计方案。安全设计方案应包含网络安全体系总体设计方案、密码应用方案、数据安全保护方案。
	2020 年 8 月	《湖南省省直单位政务信息系统项目建设管理办法》(湘政办发〔2020〕34 号)	第三章“建设和资金管理”第十六条中提出:项目建设单位应当落实国家密码管理有关法律法规和标准规范要求,同步规划、同步建设、同步运行密码保障系统并定期进行评估。未进行密码应用安全评估或评估不合格的项目,不得通过项目验收,不得投入运行。
广东省	2023 年 2 月	《关于印发〈广东省促进商用密码产业高质量发展的行动计划〉的通知》(粤密码局发〔2023〕2 号)	广东省密码管理局等 16 个部门联合印发该行动计划,进一步强调“重要网络和信息运营者同步规划、同步建设、同步运行密码保障系统,定期开展商用密码应用安全性评估并及时对结果进行备案”等要求。
	2022 年 12 月	《关于进一步规范商用密码应用安全性评估试点工作的通知》(粤密码局发〔2022〕13 号)	按照国家密码管理局有关文件要求,为进一步规范商用密码应用安全性评估各相关主体责任、密评工作流程以及监管工作要求等,广东省密码管理局印发该通知。
	2021 年 12 月	《关于规范商用密码应用安全性评估结果备案工作的通知》(粤密码协调组〔2021〕7 号)	按照国家密码管理局有关文件要求,为规范商用密码应用安全性评估备案工作,广东省密码应用推进工作协调小组办公室印发该通知。
	2021 年 3 月	《广东省发展改革委 广东省政务服务数据管理局关于印发〈广东省涉及固定资产投资的省级政务信息化项目审批细则〉的通知》(粤发改高技函〔2021〕566 号)	在粤府办〔2020〕9 号文件基础上,进一步明确涉及固定资产投资的省级政务信息化项目的密码应用及商用密码应用安全性评估要求。
	2020 年 6 月	《广东省政务服务数据管理局关于印发〈广东省省级政务信息化服务项目立项审批细则〉的通知》(粤政数〔2020〕12 号)	在粤府办〔2020〕9 号文件基础上,进一步明确项目立项前对密码应用方案进行商用密码应用安全性评估等要求和流程。

省(自治区、直辖市)、新疆生产建设兵团	发布时间	政策文件	相关内容
广东省	2020年6月	《广东省政务服务数据管理局关于印发〈广东省省级政务信息化服务项目验收前符合性审查细则〉的通知》(粤政数〔2020〕13号)	在粤府办〔2020〕9号文件基础上,进一步明确项目验收前对系统进行商用密码应用安全性评估等要求和流程。
	2020年6月	《广东省省级政务信息化项目商用密码应用工作指引》(粤密码协调组〔2020〕2号)	在粤府办〔2020〕9号、粤政数〔2020〕12号、粤政数〔2020〕13号文件基础上,广东省密码应用推进工作协调小组办公室印发该指引,进一步明确项目规划、建设、运行等各阶段密码应用和商用密码应用安全性评估工作要求、流程;并根据最新政策和标准要求不断优化完善,分别于2021年9月修订(粤密码协调组〔2021〕4号)、2021年12月印发补充通知(粤密码协调组〔2021〕5号)、2022年9月修订(粤密码协调组〔2022〕6号)。
	2020年4月	《广东省人民政府办公厅关于印发广东省省级政务信息化项目管理办法的通知》(粤府办〔2020〕9号)	“涉及密码应用的项目应当落实国家密码管理有关法律法规和标准规范的要求,同步规划、同步建设、同步运行密码保障系统并定期进行评估”。“不符合密码应用和网络安全要求的项目不予立项”。
广西壮族自治区	2022年9月	《关于加快数字化转型发展深入推进数字广西建设的实施意见》(桂发〔2022〕18号)	第一章“总体要求”第二条中提出:确保发展安全可控。统筹发展和安全,坚持促进发展与监管规范并重,建立健全安全管理体系、技术防护体系和协同监管体系,强化网络安全、关键信息基础设施安全、数据资源安全,全方位提升安全防护能力。 重点任务清单第四条“构筑数字广西‘新基座’”中提出:健全网络安全等级保护、信息系统分级保护、密码应用安全性评估、风险评估、预警和应急处置制度,推动行业组织建立健全本行业的网络安全保护规范和协作机制。
	2021年12月	《广西政务信息化发展“十四五”规划》(公开版)(桂发改高技〔2021〕1196号)	创新密码技术和应用,强化密码安全管理和综合服务,加强密码应用测评能力建设,推进密码在政务信息化建设中全面有效应用。
	2021年3月	《广西壮族自治区政务信息化项目建设管理办法(试行)》(桂政办发〔2021〕21号)	第四章“建设和资金管理”第十九条中提出:项目建设单位应当落实国家密码管理有关法律法规和标准规范的要求,同步规划、同步建设、同步运行密码保障系统并定期进行评估。
海南省	2022年11月	《省本级政务信息化项目验收管理规范(暂行)》(琼数组办〔2022〕10号)	省政务信息化项目主管部门会同省委网信办、省发展改革委、省密码局等相关部门组织竣工验收。明确将商用密码应用安全性评估作为项目竣工验收的前置必备条件,密评报告作为项目验收必备材料,省密码局专家代表在项目竣工验收评审会上具有一票否决权。



省(自治区、直辖市)、新疆生产建设兵团	发布时间	政策文件	相关内容
海南省	2022 年 9 月	《海南省电子政务云密码服务管理办法(试行)》(琼数建〔2022〕46 号)	进一步规范全省电子政务云上信息系统商用密码应用和管理,依托省电子政务云密码服务平台为全省各级政务部门提供集约高效的密码服务。
	2022 年 7 月	《海南省政务信息化项目建设管理实施细则(暂行)》(琼数组办〔2022〕5 号)	新建项目的网络安全设计应包括安全管理制度建设、入网安全评估、等级保护测评、渗透测试、安全加固等安全内容。运维类项目应按需规划网络安全等级保护测评、商用密码应用安全性评估、信息系统风险评估、应急演练、重要活动保障等网络安全保障服务内容,保障信息系统安全稳定运行。
	2022 年 7 月	《海南省促进商用密码应用和产业发展若干政策措施》(琼国密局字〔2022〕12 号)	着眼自贸港建设风险防控需要,围绕自贸港封关运作准备工作大局,从统筹规范政务领域密码应用、推进重要领域和关键信息系统密码应用、鼓励科研创新和加强人才培养、支持培育企业和促进产业发展等几个方面共提出了 15 条针对性的政策措施。
	2022 年 6 月	《海南省政务信息化项目投资编制标准(试行)》(琼数政〔2022〕28 号)	第二章“建设类项目费用投资测算标准”第二节“项目建设其他费”第七条“商用密码应用安全性评估费”中明确提出:商用密码应用安全性评估费的定义、费用范围、计取方法和标准等。
	2021 年 3 月	《关于进一步明确省政务信息化项目建设密码应用有关要求的通知》(琼国密局字〔2021〕2 号)	第五条、第七条中提出:新建、改建、扩建以及通过政府购买服务产生的政务信息化项目,项目建设单位在项目建设完成后,应委托评估机构对信息系统进行密码应用安全性评估。政务信息系统投入运行后,建设单位应按照国家密码管理有关法规要求定期委托评估机构对系统开展密码应用安全性评估,并根据安全需求、风险威胁程度、系统环境变化以及对系统安全认识的深化持续改进密码保障措施。
	2020 年 12 月	《海南省政务信息化项目建设管理办法》(琼府办〔2020〕38 号)	第二章“规划和审批管理”第八条中提出:省级各部门产生的政务信息化项目,省大数据管理局应当按规定履行审批程序并向省发展改革委备案。备案文件应当包括项目名称、建设单位、审批部门、绩效目标及绩效指标、投资额度、运行维护经费、经费渠道、信息资源目录、信息共享开放、应用系统、等级保护或者分级保护备案情况、密码应用方案和密码应用安全性评估报告等内容,其中改建、扩建项目还需提交前期项目第三方后评价报告。
重庆市	2022 年 2 月	《关于规范重庆市市级政务信息化项目密码应用有关要求的通知》(渝密局〔2022〕1 号)	进一步明确市级政务化项目各阶段密码应用要求:项目规划阶段应按照相关标准编制密码应用方案,并对方案进行评审;项目建设阶段应严格按照通过评审的方案进行建设,建设完成后委托商用密码应用安全性评估机构进行评估,在商用密码应用安全性评估报告出具 30 日内报市密码局备案;项目运行阶段应开展定期评估、应急评估,统筹做好密码保障系统改造工作。

省(自治区、直辖市)、新疆生产建设兵团	发布时间	政策文件	相关内容
重庆市	2021 年 11 月	《重庆市市级政务信息化项目管理办法》(渝府办发〔2021〕122 号)	第四章“监督管理”第三十五条中提出：市级各部门应当严格遵守有关保密等法律法规规定，构建全方位、多层次、一致性的防护体系，按要求采用密码技术，并定期开展密码应用安全性评估，确保政务信息系统运行安全和政务数据资源共享交换的数据安全。
	2021 年 2 月	《关于印发重庆市工业信息安全管理实施办法(试行)的通知》	第九条提出：主体企业负有本单位工业信息安全的主体责任，应结合实际做好本单位工业信息安全防护，建立健全工业信息安全责任制，负责本单位工业信息安全保障和应急管理工作，落实人、财、物保障。主体企业负责依法落实网络安全等级保护制度，开展定级备案、等级测评、商用密码应用安全性评估和安全建设整改等工作。
四川省	2023 年 2 月	《关于委托开展商用密码应用安全性评估结果备案相关工作的通知》(川密局〔2023〕4 号)	各市(州)密码管理局受省密码管理局委托，负责本地区密评结果备案的初审转报工作。驻川机构、省直部门以及中央、省属企事业单位规划建设的信息系统可直接报省密码管理局备案。
	2022 年 10 月	《四川省省级政务信息化项目密码应用与安全性评估工作指南》(川密局〔2022〕18 号)	对四川省省级政务信息化项目在规划阶段、建设阶段、运行阶段的密码应用和密评工作要求作出具体安排，用以指导各建设单位开展工作。
	2022 年 4 月	《四川省一体化政务服务平台电子证照管理暂行办法》(川办规〔2022〕3 号)	第五章“电子印章信息安全”第二十二条中提出：电子证照系统建设单位按照“谁建设、谁负责”的原则，落实网络安全等级保护制度和国家密码应用相关要求。电子证照系统建设单位应充分利用密码技术、生物特征技术以及其他必要的安全技术手段，加强证照申请人、持证主体身份认证，确保身份真实可信。
	2022 年 4 月	《四川省一体化政务服务平台电子印章管理暂行办法》(川办规〔2022〕3 号)	第一章“总则”第六条中提出：省一体化平台电子印章系统应当符合国家有关密码标准规范，应当通过国家密码管理部门认可的商用密码应用安全性评估。
	2021 年 10 月	《四川省省级政务信息化项目管理办法》(川办发〔2021〕49 号)	第四章“建设和运维管理”第三十一条中提出：建设项目由省发展改革委组织竣工验收，验收资料包括密码应用安全性评估报告等材料。 第八章“安全管理”第四十九条中提出：省密码管理局应依法加强对政务信息系统密码应用的安全监管，指导监督项目单位规范密码应用和管理。 第八章“安全管理”第五十一条中提出：项目不符合密码应用和网络安全要求，或者存在重大安全隐患的，不安排运行维护经费，项目单位不得新建、改建、扩建政务信息系统。



省(自治区、直辖市)、新疆生产建设兵团	发布时间	政策文件	相关内容
四川省	2021年9月	《四川省“十四五”数字政府建设规划》(川府发〔2021〕24号)	第四章“夯实数字政府建设基础”第五节中提出:落实关键信息基础设施保护制度和网络安全等级保护制度,建立重大项目网络安全风险评估机制,加强密码应用安全性评估工作。 建设密码技术支撑平台,规范、完善和深化密码在政务云平台等政务服务系统的应用。 提升密码产品检测和系统分析能力,完善密码应用安全性评估审查机制,构建自主可控的密码认证测评体系。 推进基础设施网络密码应用,强化密码在信息惠民及社会治理中的应用,提升关键信息基础设施密码保障能力。
贵州省	2023年3月	《关于进一步规范商用密码应用安全性评估试点工作的通知》	指导各市州密码管理部门进一步强化职责,严格监管指导密评试点工作用户单位、密评机构,规范密评结果备案材料形式审查制度,建立完善密评结果备案材料复核制度,推动密评结果客观真实。
	2023年1月	《贵州省省级政务信息系统建设管理办法》	明确对省级政务信息系统密码应用“三同步一评估”作出明确要求,省大数据局组织相关部门,对项目建设单位报送的年度服务方案在相关政策符合性、可行性、软件架构及业务功能、数据资源建设与管理、密码运用、硬件部署方案、云资源占用合理性及投资概算等方面进行评审。
	2022年1月	《关于做好商用密码应用安全性评估结果备案工作的通知》	指导全省省直单位、中央在黔、人民团体等单位严格按照“三同步一评估”要求推进商用密码应用,规范开展商用密码应用安全性评估结果备案工作。 指导各市州密码管理部门依照分级管理要求,做好商用密码应用安全性评估结果备案管理工作,按时报送当地密评备案信息,指导督促本地网络与信息系统运营者按照“三同步一评估”要求,推进商用密码应用。
云南省	2022年5月	《云南省“十四五”电子政务发展规划》(云政办发〔2022〕37号)	第五章“筑牢立体化安全运维和标准规范体系”第一节“强化稳健可控的安全与运维保障体系”中提出:推进国产密码应用,加强国产密码基础设施集约化建设和供给。推动关键基础设施保护、等级保护、分级保护、密码应用评估等信息安全测评工作常态化。
	2022年4月	《“十四五”数字云南规划》(云政发〔2022〕26号)	第八章“营造健康安全数字生态”第二节“健全网络信息安全体系”中提出:健全网络安全防护体系。落实信息系统安全等级保护、涉密信息系统分级保护及风险评估制度,定期开展网络安全专项督查与评估。规范、完善和深化国产密码应用,提升密码基础支撑能力、建立健全密码应用安全性评估审查制度。
	2022年4月	《云南省“十四五”新型基础设施建设规划》(云政发〔2022〕28号)	第六章“促进新型基础设施开放与安全”第二节“提升安全保障水平”中提出:规范密码应用和管理,促进密码事业发展,保障网络与信息安全。支持开展网络安全技术和产品研发。

省(自治区、直辖市)、新疆生产建设兵团	发布时间	政策文件	相关内容
西藏自治区	2022 年 7 月	《西藏自治区非涉密政务信息系统商用密码应用与安全性评估工作指南(试行)》(藏密局发〔2022〕3号)	该文件用于指导和规范西藏自治区非涉密政务信息系统商用密码应用与安全性评估工作,明确了商用密码方案编制及评审、信息系统商用密码应用安全性评估、商用密码应用安全性评估备案等业务流程和管理要求。
	2022 年 4 月	《西藏自治区政务信息化项目建设管理办法》(藏政办发〔2022〕14号)	第三章“建设和资金管理”第十五条中提出:项目建设单位应当落实国家密码管理有关法规和标准规范的要求,同步规划、同步建设、同步运行密码保障系统并定期进行评估。
	2021 年 12 月	《关于规范商用密码应用安全性评估结果备案工作的通知》(藏密局发〔2021〕4号)	该文件提出商用密码应用安全性评估结果备案的具体要求。
陕西省	2023 年 2 月	《关于征求陕西省数字政府建设 2023 年工作要点(征求意见稿)》	第四章“全面筑牢网络安全的坚固防线”第十五条“完善安全管理制度规范”中提出:完善省级数字政府网络安全制度规范体系,制定……密码应用等相关安全测评。
	2022 年 9 月	《陕西省省级政务信息化建设专项资金管理办法》	进一步加强省级政务信息化建设专项资金管理,将密码应用安全性评估经费纳入项目申报预算…确保专项资金安全运行、专款专用。
	2022 年 6 月	《陕西省省级政务信息化项目建设管理办法(暂行)》(陕政办发〔2022〕19号)	第一章“总则”第三条中提出:省委网信办、省公安厅、省国家保密局、省国家密码管理局、省审计厅等按照职责分工,负责项目网络安全监管、等级保护、分级保护、密码评估、审计监督等相关工作。
	2021 年 10 月	《陕西省人民政府办公厅关于印发数字政府建设“十四五”规划的通知》陕政办发〔2021〕27号	第三章“主要任务”第三节“三大运行保障”中提出:加强政务数据全生命周期管理,制定完善政务数据安全管理制度和数据分类分级、共享开放、使用销毁等管理制度。落实等级保护、商用密码应用安全性评估等合规性要求。
甘肃省	2022 年 4 月	《甘肃省人民政府办公厅关于加快推进电子证照扩大应用领域和互通互认的通知》(甘政办发〔2022〕50号)	第二章“全面落实工作任务”第十条中提出:强化电子证照安全管理。各地各部门要做好电子证照系统日常运行维护,定期开展网络安全等级保护测评、密码应用安全性评估等工作。
	2021 年 12 月	《甘肃省数字政府建设总体规划(2021-2025)》(甘政办发〔2021〕113号)	第四章“主要任务”第五节“推进体系建设,完善数字政府运行新机制”第二条“构建可管可信的安全保障体系”中提出:落实安全技术手段支撑。逐步推进安全技术手段建设,同步规划、同步建设、同步运行密码保障系统并定期进行评估,形成覆盖政务云、网、大数据基座、政务业务应用的安全保障技术支撑能力。
	2021 年 9 月	《甘肃省“十四五”数字经济创新发展规划》(甘政办发〔2021〕88号)	保障数据安全。落实等级保护、密码应用、安全测评、密码测评、电子认证、应急管理基础制度。



省(自治区、直辖市)、新疆生产建设兵团	发布时间	政策文件	相关内容
青海省	2020 年 5 月	《关于印发青海省省级政务信息化项目建设管理办法的通知》(青政办〔2020〕38 号)	第三章“建设和资金管理”第十八条中提出:项目建设单位应当落实国家网络安全和密码管理有关法律法规和标准规范的要求,同步规划、同步建设、同步运行网络安全和密码保障系统并定期进行评估。 第四章“监督管理”第三十三条中提出:各部门应当严格遵守有关保密等法律法规规定,构建全方位、多层次、一致性的防护体系,按要求采用密码技术,并定期开展密码应用安全性评估,确保政务信息系统运行安全和政务信息资源共享交换的数据安全。
宁夏回族自治区	2023 年 1 月	《关于进一步规范全区商用密码应用安全性评估工作的通知》	进一步强化密评主体责任,加强对密评实施活动的监督,规范密评结果备案工作,严格开展形式审查,鼓励商密协会发挥作用,加强行业自律,促进行业健康发展。
	2022 年 5 月	《关于进一步规范全区政务信息化项目商用密码应用和安全性评估的通知》(宁密局发〔2022〕1 号)	项目建设单位应落实国家密码管理有关法律法规和标准规范的要求,使用商用密码进行保护,同步规划、同步建设、同步运行密码保障系统并定期开展密码应用安全性评估。 在项目规划阶段,应制定密码应用方案,并委托评估机构对方案开展密码应用安全性评估。未通过密评的密码应用方案,不得作为密码保障系统的建设依据;项目建设完成后,应委托评估机构开展密码应用安全性评估。信息系统投入运行后,项目建设单位应委托评估机构每年对系统开展密码应用安全性评估,确保密码保障系统正确有效运行。关键信息基础设施和网络安全等级保护第三级系统应在 2022 年底前完成,未完善密码保障系统并通过评估的,第二年起不予安排运维经费,并暂停安排除密码保障系统建设完善之外的信息化项目。
	2021 年 12 月	《关于规范我区商用密码应用安全性评估结果备案工作的通知》(宁密局发〔2021〕1 号)	网络与信息系统密评备案主体应为各地区各部门网络与信息系统运营者,各责任单位务必高度重视,认真履行密码安全主体责任,明确密码安全负责人,按要求开展密评、备案和密码应用整改,配合密码管理部门和有关部门的安全检查。
	2021 年 8 月	《宁夏电子政务建设十四五规划意见》	1)严格落实密码应用安全性评估制度,强化全网、全域、全业务的电子政务综合安全防护。2)升级优化电子政务信息服务体系,为电子政务资源安全利用和行为可信提供安全支持保障。3)完善电子政务密码保障体系,促进电子政务公共云平台密码服务能力建设,为云上应用提供集约化密码服务,实现密码在电子政务系统中的有效应用。

省(自治区、直辖市)、新疆生产建设兵团	发布时间	政策文件	相关内容
宁夏回族自治区	2021年6月	《宁夏回族自治区贯彻落实网络安全等级保护制度和关键信息基础设施安全保护制度的实施意见》(宁公(网安)通〔2021〕42号)	网络运营者要认真贯彻落实《中华人民共和国密码法》等有关法律法规规定和密码应用相关标准规范。新建第三级(含)以上网络,运营者要按照“三同步”的要求正确、有效采用密码技术对网络系统进行保护,并使用符合相关法律法规规定的密码产品和服务,已运行的第三级(含)以上网络运营者要尽快按要求进行整改。第三级(含)以上网络运营者要在网络规划、建设阶段同步规划密码防护措施,在网络安全等级测评中同步开展密码应用安全性评估,正式运行后,每年至少评估一次。评估完成后,应在30个工作日内将评估结果报所在地密码管理部门、公安部门备案。
新疆维吾尔自治区	2023年2月	《新疆维吾尔自治区密码管理局关于进一步规范自治区商用密码应用建设和安全性评估工作的通知》(新机发明电〔2023〕1号)	第二章“规范开展密码应用安全性评估”中提出:“明确范围。网络安全等级保护三级以上的网络和信息系统的应开展商用密码应用安全性评估。其中采取租赁云平台部署的信息系统(如门户网站等)应独立可进行评估;采取组网或终端方式接入上级部门建设的重要信息系统的,若具备本地接入用户、系统运维管理等实质全线,或在本地进行系统数据汇集、系统分中心部署等实质控制行为,应独立进行评估。”“确保客观。各地各部门应采取直接委托具备资质的第三方测评机构开展商用密码应用安全性评估,不得委托信息系统集成商全权代理,不得干扰第三方测评机构独立自主开展工作,不得影响干预评估结果。”
	2023年2月	《新疆维吾尔自治区公共数据管理办法(试行)》(新政办发〔2023〕11号)	第七章“监督保障”第三十八条中提出:公共数据提供部门、公共数据使用部门、平台建设运维管理部门应遵循“谁提供、谁负责,谁使用、谁负责,谁流转、谁负责”的原则,按照国家信息安全等级保护、数据分类分级管理、密码应用安全保护要求,在公共数据资源共享开放全过程中加强安全传输、访问控制、授权管理、全流程审计等方面的安全管理和防护。
	2021年2月	《新疆维吾尔自治区密码管理局关于深入贯彻密码法进一步健全完善自治区密码应用和管理工作机制的指导意见》(新密局〔2021〕4号)	第二节“建立完善密码应用工作报告机制”中提出:“责任单位要将密码应用管理工作纳入项目建设各环节。规划阶段:责任单位应依据密码应用有关标准,制定商用密码应用建设方案,组织专家或委托测评机构进行评估论证,论证结果作为必要条件列入项目立项材料并报本级密码管理部门备案。建设阶段:责任单位应当委托第三方测评机构进行商用密码应用安全性评估,评估结果作为项目验收重要依据并报本级密码管理部门备案。运行阶段:定期开展商用密码应用安全性评估,评估报告报本级密码管理部门备案。 第四节“建设完善密码应用联合审查机制”中提出:“4.项目验收阶段,密码应用安全性评估报告是项目验收的必要条件。对于不符合密码应用和网络安全防护要求,或者存在重大安全隐患的政务信息系统,不安排运行维护经费,项目建设单位不得新建、改建、扩建信息系统。”



省(自治区、直辖市)、新疆生产建设兵团	发布时间	政策文件	相关内容
新疆维吾尔自治区	2021 年 2 月	《新疆维吾尔自治区政务信息化项目建设管理办法》(新政办发〔2021〕14 号)	第十四条提出:项目建设单位应当落实《中华人民共和国密码法》,自治区密码管理有关法规规章和标准规范要求,同步规划、同步建设、同步运行密码保障系统并定期进行评估。 第二十八条提出:……各部门应当严格遵守有关保密等法律法规规定,构建全方位、多层次、一致性的防护体系,按要求采用密码技术,并定期开展密码应用安全性评估,确保政务信息系统运行安全和政务信息资源共享交换的数据安全。
新疆生产建设兵团	2021 年 12 月	《兵团办公厅关于印发<兵团政务信息化项目建设管理办法(试行)>的通知》(新兵办发〔2021〕126 号)	第七章“安全管理”第四十七条中提出:项目建设单位应落实国家网络安全、数据安全、个人信息保护、密码管理有关法律法规和标准规范的要求,建立网络安全、数据安全制度,加强政务信息系统与信息资源系统的安全保密设施建设,同步规划、同步建设、同步运行网络安全、密码保障系统并定期进行检测和评估。

附录 2: 密评相关标准与指导性文件列表

查阅相关国家标准请访问全国信息安全标准化技术委员会网站: <https://www.tc260.org.cn/>, 查阅相关行业标准请访问密码行业标准化技术委员会网站: <http://www.gmbz.org.cn>。

表 7 密评相关标准列表

序号	标准编号	标准名称	备注
1	GB/T 39786-2021	信息安全技术 信息系统密码应用基本要求	已发布
2	GM/T 0115-2021	信息系统密码应用测评要求	已发布
3	GM/T 0116-2021	信息系统密码应用测评过程指南	已发布
4	-	信息安全技术 信息系统密码应用测评要求	在研
5	-	信息安全技术 信息系统密码应用设计技术指南	在研
6	-	信息系统密码应用实施指南	在研
7	-	商用密码应用安全性评估机构能力要求和评价规范	在研
8	-	商用密码应用安全性评估监督检查规范	在研
9	-	信息系统密码安全管理体系	在研

查阅密评指导性文件请访问中国密码学会网站：<https://www.cacnet.org.cn>。

表 8 密评指导性文件列表

序号	文件名称	备注
1	信息系统密码应用高风险判定指引	已发布
2	商用密码应用安全性评估量化评估规则	已发布
3	商用密码应用安全性评估报告模板(2023 版)—方案密评报告	已发布
4	商用密码应用安全性评估报告模板(2023 版)—系统密评报告	已发布
5	商用密码应用安全性评估 FAQ(第二版)	已发布

附录 3：密评大事记

2017 年 4 月，根据《关于开展密码应用安全性评估试点工作的通知》（国密局字〔2017〕138 号）的工作部署，国家密码管理局启动密评试点。

2017 年 11 月，组织全国第一批密评人员培训考核工作，经过严格的机构遴选和人员培训考核机制，认定了第一批 27 家密评试点机构，并于 2018 年 6 月向推荐省部印发《商用密码应用安全性测评机构目录》。

2018 年 2 月，密码行业标准化技术委员会发布 G M /T 0054-2018 《信息系统密码应用基本要求》，对信息系统中如何应用密码提出了基本要求，指导、规范和评估信息系统中的商用密码应用。

2019 年 3 月，国家密码管理局商用密码检测中心等六家密评机构的主要负责人共同发起倡议成立密评联委会，加强密评机构自我管理及行业自律，推动密评机构之间的合作，共同促进测评技术和标准创新发展。

2019 年 6 月 3-4 日，密评联委会工作启动暨技术交流培训会议在京召开。

2019 年 10 月 26 日，十三届全国人大常委会第十四次会议通过《中华人民共和国密码法》，习近平主席签署第 35 号主席令予以公布。

2019 年 11 月 1 日，第三届中国密码学会常务理事会审议通过《中国密码学会商用密码应用安全性评估联合委员会工作条例》，密评联委会组织体系得到进一步健全。

2020 年 1 月 13 日至 17 日，密评联委会支撑国家密码管理局开展第二批密评试点机构相关从业人员培训工作。

2020 年 6 月 30 日，密评联委会支撑国家密码管理局开展密评试点机构能力验证。随后，国家密码管理局发布第 40 号公告，发布《商用密码应用安全性评估试点机构目录》（共收录 24 家机构）。

2020 年 9 月 16 日，密评联委会组织编制的《政务信息系统密码应用与安全性评估工作指南》(2020 版)正式发布。

2020 年 12 月，密评联委会发布《信息系统密码应用测评要求》《信息系统密码应用测评过程指南》《信息系统密码应用高风险判定指引》《信息系统密码应用安全性评估量化评估规则》以及《商用密码应用安全性评估报告模板（2020 版）》等 5 项商用密码应用与安全性评估指导性文件。



2021年1月8日，由密评联委会主办的密评工作研讨会通过远程会议方式召开，研讨会旨在宣贯最新密码相关法律法规和标准要求，进一步统一规范密评机构测评活动，加强密评机构经验交流，提高密评机构能力水平。

2021年3月19日，国家市场监督管理总局、国家标准化管理委员会发布公告，正式发布国家标准 GB/T 39786-2021《信息安全技术 信息系统密码应用基本要求》。

2021年5月，密评联委会支撑国家密码管理局开展第二批密评试点机构能力考核。

2021年6月，国家密码管理局发布第42号公告，更新《商用密码应用安全性评估试点机构目录》（共收录48家机构）。

2021年10月22日，密评联委会党小组会议审议了密评联委会组织架构设置与主要职责，决定设置总体组、标准支撑组、能力建设组、行业促进组等4个小组，分别负责总体设计、标准供给、能力建设、行业自律等相关工作。

2021年10月，国家密码管理局发布第43号公告，发布 GM/T 0115-2021《信息系统密码应用测评要求》等15项密码行业标准，为密评工作的深入开展提供标准支撑。

2021年11月，国家密码管理局印发《关于规范商用密码应用安全性评估结果备案工作的通知》，进一步规范密评工作。

2021年12月，密评联委会修订的《信息系统密码应用高风险判定指引》《商用密码应用安全性评估量化评估规则》《商用密码应用安全性评估报告模板（2021版）》等3项商用密码应用与安全性评估指导性文件及《商用密码应用安全性评估 FAQ》（常见问题解答）正式发布。

2022年7月8日，密评联委会支撑国家密码管理局开展密评试点机构测评人员线上考核。

2022年9月29日，由密评联委会主办、中国电力科学院承办的《商用密码应用安全性评估 FAQ（第二版）》技术培训在线上举行，共2300余人参加培训。

2022年12月1日，国家密码管理局印发了《关于进一步规范商用密码应用安全性评估试点工作的通知》，进一步加强对密评试点工作的督促指导。

2023年1月，密评联委会更新发布《商用密码应用安全性评估报告模板（2023版）》，用于替代2021年12月发布的《商用密码应用安全性评估报告模板（2021版）》。

2023年4月27日，李强总理签署第760号国务院令，公布修订后的《商用密码管理条例》，2023年7月1日起正式施行。

2023年6月9日，《商用密码检测机构管理办法（征求意见稿）》和《商用密码应用安全性评估管理办法（征求意见稿）》向社会公开征求意见。

2023年7月17日，密评联委会更新发布《商用密码应用安全性评估量化评估规则（2023版）》，用于替代2021年12月发布的《商用密码应用安全性评估量化评估规则》。