**密码政策问答**

国家密码管理局

《中华人民共和国密码法》已于2020年1月1日正式施行，为做好政策解释，引导社会各界更好地贯彻落实《密码法》，国家密码管理局特制定“密码政策问答”，发布于国家密码管理局网站“信息公开”板块的“政策解读”栏目。以下为具体问答内容（更新至2020年5月6日）。

**1.问：《密码法》施行后，商用密码产品的管理方式有什么变化?**

答：根据《密码法》第二十五条、第二十六条的规定，商用密码产品管理方式将由行政审批调整为检测认证管理，国家密码管理局不再实施“商用密码产品品种和型号审批”。市场监管总局会同国家密码管理局建立国家统一推行的商用密码认证制度，采取支持措施，鼓励商用密码产品获得认证。对列入网络关键设备和网络安全专用产品目录的商用密码产品实施强制性检测认证，由具备资质的机构检测认证合格后，方可销售或者提供。

**2.问：《密码法》施行后，已发放的《商用密码产品型号证书》是否有效?**

答：《密码法》施行后，市场监管总局将会同国家密码管理局建立国家统一推行的商用密码认证制度，国家密码管理局将不再受理商用密码产品品种和型号申请，停止发放《商用密码产品型号证书》，已发放的《商用密码产品型号证书》自2020年7月1日起自动失效。本着便民利企原则，对于在有效期内的《商用密码产品型号证书》，持证单位可于2020年6月30日前自愿申请转换国推商用密码产品认证证书，换发的认证证书有效期与原《商用密码产品型号证书》有效期保持一致。同时，为方便证书转换，持证单位可向所在地省(区、市)密码管理部门提交转换认证申请。

**3.问：《密码法》施行后，尚未完成商用密码产品品种和型号审批的产品应该如何处理?**

答：本着便民利企原则，对于尚未完成商用密码产品品种和型号审批的，原产品品种和型号申请单位可于2020年6月30日前，自愿转为认证申请；审批期间已经开展的审查及检测，认证机构不再重复审查、检测，切实减轻申请单位负担，简化办事流程。

**4.问：《密码法》施行后，如何向具备资质的商用密码认证机构提交认证申请?**

答：市场监管总局、国家密码管理局正在抓紧制定国推商用密码认证的产品目录、认证规则和有关实施要求。待相关内容发布后，自认证规则实施之日起，商用密码从业单位便可自愿向具备资质的商用密码认证机构提交认证申请。有关认证的适用范围、申请受理、基本流程、证书管理等内容将在认证规则中予以明确。

**5.问：《密码法》施行后，商用密码进出口有哪些管理要求?**

答：根据《密码法》第二十八条的规定，《密码法》施行后，商用密码进出口将纳入两用物项进出口管理，由商务部、国家密码管理局依法实施进口许可和出口管制。商务部、国家密码管理局、海关总署正在抓紧制定商用密码进口许可清单和出口管制清单。清单公布实施前，商用密码进出口暂时按照目前公布的许可条件和程序实施进出口许可管理，保持现行工作方式不变。详见国家密码管理局、商务部、海关总署第38号公告。

**6.问：《密码法》中“密码”的概念是什么?**

答：《密码法》中的密码(cryptography)，是指采用特定变换的方法对信息等进行加密保护、安全认证的技术、产品和服务。而人们日常接触的计算机或手机开机“密码”、微信“密码”、QQ“密码”、电子邮箱登录“密码”、银行卡支付“密码”等，实际上是口令(password)。口令是进入个人计算机、手机、电子邮箱或银行账户的“通行证”，是一种简单、初级的身份认证手段，“口令”不在《密码法》的管理范围之内。

**7.问：《密码法》有什么样的法律地位?**

答：密码是国家重要战略资源，是保障网络与信息安全的核心技术和基础支撑。密码工作是党和国家的一项特殊重要工作，直接关系国家政治安全、经济安全、国防安全和信息安全，在我国革命、建设、改革各个历史时期，都发挥了不可替代的重要作用。进入新时代，以习近平同志为核心的党中央坚持总体国家安全观，在完善国家安全体系的总体布局中对加强密码工作和密码立法作出了重要部署。

《密码法》是我国国家安全法律制度体系的重要组成部分，是密码领域的综合性、基础性法律，也是一部技术性、专业性较强的专门法律。《密码法》以法律的形式明确了党管密码的根本原则，确立了密码工作领导和管理体制，明确了密码分类管理原则以及核心密码、普通密码、商用密码管理的各项制度措施，为保障网络与信息安全，维护国家安全、社会公共利益，以及公民、法人和其他组织的合法权益提供了坚实有力的法律保障，为构建系统完备、科学规范、运行高效的密码法律制度体系奠定了基础。

**8.问：《密码法》的立法目的是什么?**

答：一、规范密码应用和管理，促进密码事业发展

目前，有关部门、单位和社会公众对密码的作用认识不够全面，使用密码保护网络与信息安全的意识还不够强，特别是重要网络与信息系统密码应用规范性、有效性不够的问题还比较突出，严重威胁国家网络与信息安全、企业商业秘密以及公民个人隐私保护。国家对涉密信息系统和关键信息基础设施商用密码的应用、基础支撑能力的提升以及安全性评估、审查制度等不断提出明确要求，需要上升为法律规范，为维护国家网络与信息安全提供法治保障。在核心密码、普通密码方面，需要将现行有效的安全管理制度、特殊管理政策及保障措施法治化，增强核心密码、普通密码安全保障能力。在商用密码方面，传统上对商用密码实行全环节许可管理，已经不适应政府职能转变和“放管服”改革要求，亟需通过立法对现行的商用密码管理制度作出调整，切实为企业松绑减负，促进密码科技进步和创新，促进密码产业健康有序发展。

二、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

在网络与信息时代，每天都会产生大量涉密和敏感信息，网络窃密、网络诈骗、侵犯隐私等事件层出不穷，亟需有效的安全防护措施。密码是保障网络与信息安全的核心技术和基础支撑。制定《密码法》，就是要更好地促进密码产业发展，营造良好的市场秩序，为社会提供更多优质高效的密码，引导全社会正确、合规、有效使用密码，充分发挥密码在网络空间中信息加密、安全认证等方面的重要作用，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。

**9.问：《密码法》经历了怎样的立法过程?**

答：党和国家高度重视密码立法工作，2018年至2019年，全国人大常委会和国务院都将《密码法》列入了立法工作规划。

2014年12月，国家密码管理局正式启动《密码法》的立法工作。

2017年4月至5月，《中华人民共和国密码法(草案征求意见稿)》在国家密码管理局商用密码管理办公室网站首次面向社会公开征求意见。

2017年6月，《中华人民共和国密码法(草案送审稿)》正式报送国务院。

2019年6月10日，《中华人民共和国密码法(草案)》(以下简称草案)经国务院第52次常务会议会讨论通过。6月15日，李克强总理签署议案，正式将草案提请全国人大常委会审议。

2019年6月25日至29日，十三届全国人大常委会第十一次会议对草案进行了首次审议。

2019年7月5日至9月2日，草案在中国人大网面向社会公开征求意见。

2019年10月21日至26日，十三届全国人大常委会第十四次会议对草案进行了二次审议。

10月26日，十三届全国人大常委会第十四次会议表决通过《密码法》，习近平主席签署第三十五号主席令正式颁布，自2020年1月1日起施行。

**10.问：密码有哪些主要功能?**

答：密码的主要功能有两个，一个是加密保护，另一个是安全认证。

加密保护是指采用特定变换的方法，将原来可读的信息变成不能直接识别的符号序列。简单地说，加密保护就是将明文变成密文。例如，古希腊军队使用一种叫做“斯巴达棒”的圆木棍来进行加密通信，使用方法是：把一根长带状羊皮纸缠绕在圆木棍上，然后在上面写字；解下羊皮纸后，上面只有乱序的字符，只有再次以同样的方式缠绕到同样粗细的木棍上，才能看出所写的内容。

安全认证是指采用特定变换的方法，确认信息是否完整、是否被篡改、是否可靠以及行为是否真实。简单地说，安全认证就是确认主体和信息的真实可靠性。例如，增值税防伪税控系统采用商用密码技术保护涉税信息，增值税发票信息经密码算法进行加解密处理，确定该发票的明文信息是否真实，从而遏制增值税犯罪，减少税款流失。

**11.问：《密码法》的管理对象有哪些?**

答：作为本法的管理对象，密码包括密码技术、密码产品和密码服务。

密码技术，是指采用特定变换的方法对信息等进行加密保护、安全认证的技术，包括密码编码、实现、协议、安全防护、分析破译，以及密钥产生、分发、传送、使用、销毁等技术。分组密码算法(如SM4算法)、公钥密码算法(如SM2算法)等是典型的密码算法，密钥交换协议、密钥分发协议等是典型的密码协议。

密码产品，是指采用密码技术并以加密保护、安全认证的产品，即承载密码技术、实现密码功能的实体。典型的密码产品包括：密码机，如链路密码机、网络密码机、服务器密码机、传真密码机、电话密码机等；密码芯片和模块，如第二代居民身份证、智能电卡、社会保障卡、金融芯片卡中使用的密码芯片、可信计算密码模块等。

密码服务，是指基于密码专业技术、技能和设施，为他人提供集成、运营、监理等密码支持和保障的活动，即基于密码技术和产品，实现密码功能，提供密码保障的行为。典型的密码服务包括：密码保障系统集成(如数字证书认证系统集成)，是指为他人集成建设实现密码功能的系统，保护他人网络与信息系统的安全；密码保障系统运营(如增值税发票防伪税控系统运营)，是指为保证他人实现密码功能系统的正常运行提供安全管理和维护。

**12.问：密码工作的基本原则是什么?**

答：总体国家安全观要求推动建立新的安全体制，在密码工作中具体体现为统一领导、分级负责，创新发展、服务大局，依法管理、保障安全的基本原则，这是密码工作历史经验和实践的深刻总结。

**13.问：密码工作的基本原则中“统一领导、分级负责”是指什么?**

答：“统一领导、分级负责”是密码工作的首要原则。统一领导，是指全国密码工作在党中央领导下，由中央密码工作领导机构统一领导。《密码法》把“统一领导”作为密码工作的一项基本原则，就是要坚持党的绝对领导，这是密码工作最重要、最根本、最核心的原则，也是密码工作的优良传统和宝贵经验。

分级负责，是指国家和省、市、县四级密码管理部门分别负责管理全国和本行政区域的密码工作。根据密码工作的现实需要，参考其他工作领域管理体制改革发展的经验，《密码法》明确了各级密码管理部门的行政主体地位，确立了分级负责的密码工作管理体制。

**14.问：密码工作的基本原则中“创新发展、服务大局”是指什么?**

答：创新发展是密码工作的发展之基、力量之源。党的密码工作从诞生的第一天起，正是凭借不断地自主创新，走出了一条从无到有、从小到大、从弱到强的中国特色密码发展之路。坚持创新发展，就是要以科技创新为核心，以管理创新为推动，以制度创新为保证，支持密码科学技术研究，推动密码产业发展，使密码工作始终体现时代性、把握规律性、富于创造性，为保障网络与信息安全、维护国家网络空间主权提供有力的技术支撑。

服务大局是密码工作的价值所在，更是其宗旨要求。密码工作与党和国家的事业血肉相连、命运休戚相关，在革命、建设和改革各个历史时期，都紧紧围绕党和国家的中心任务和奋斗目标，发挥着不可替代的特殊重要作用。进入新时代，坚持服务大局，就是要紧紧围绕国家创新驱动发展战略，部署好密码科技自主创新，实现密码科技跨越式发展；要紧紧围绕国家安全战略，加大密码核心关键技术攻关和密码应用，充分发挥密码在保安全促发展中的支撑作用；要紧紧围绕中央全面深化改革的战略部署，全面深化密码管理体制改革，加快政府职能转变；要紧紧围绕经济结构调整，加快推进密码产业发展，为经济社会持续健康发展，为实现“两个一百年”奋斗目标、实现中华民族伟大复兴的中国梦做出贡献。

**15.问：密码工作的基本原则中“依法管理、保障安全”是指什么?**

答：党的十九大把坚持全面依法治国确立为习近平新时代中国特色社会主义思想和新时代坚持和发展中国特色社会主义的基本方略的重要内容，提出“必须坚持厉行法治，推进科学立法、严格执法、公正司法、全民守法”。将密码管理的各个方面纳入法治轨道，是密码工作的基本要求，是提高密码工作科学化、规范化、制度化水平的必由之路。坚持依法管理，就是各级密码管理部门要严格按照《密码法》和有关法规、规章和规范性文件的规定，依法全面履行密码行政管理职能。依法管理是核心密码、普通密码、商用密码三类密码管理的共同要求。密码安全关乎党和国家的根本利益，是密码工作的生命。坚持保障安全，就是要加强密码安全制度建设，完善密码安全管理措施，对密码管理重点关键环节实施有效监管，增强密码安全保障能力；要加强关键信息基础设施密码应用监管，建立完善密码安全性评估和安全审查制度，有效预防和化解密码安全风险；要加强密码安全协作机制建设，确保密码安全管理的协同联动和有序高效。

**16.****问：密码工作坚持党的绝对领导体现在哪些方面?**

答：坚持党对密码工作的绝对领导，是在任何时候、任何情况下都必须毫不动摇坚持的根本原则。《密码法》规定，坚持中国共产党对密码工作的领导，旗帜鲜明地把党管密码这一根本原则写入法律。党的密码工作创建于1930年，一直由党中央直接领导和管理，党管密码原则是密码工作长期实践和历史经验的深刻总结，是密码工作最重要、最根本、最核心的要求。

坚持党的绝对领导，主要体现在：一是密码工作的重大事项向中央报告，密码工作的重大决策由中央决定。二是坚决贯彻执行中央关于密码工作的方针政策，落实中央确定的密码工作领导和管理体制。三是充分发挥党的领导核心作用，各级党委(党组)和密码工作领导机构要认真履行党管密码的政治责任。

**17.问：我国的密码工作领导体制是什么?**

答：《密码法》明确规定，中央密码工作领导机构，即中央密码工作领导小组，对全国密码工作实行统一领导，把中央确定的密码工作领导体制，通过法律形式固化下来，为密码工作沿着正确方向发展提供根本保证。中央密码工作领导小组统一领导全国密码工作，负责制定国家密码工作重大方针政策，统筹协调国家密码重大事项和重要工作，推进国家密码法治建设。

**18.问：我国的密码工作管理体制是什么?**

答：根据密码工作依法管理的需要，参考其他工作领域管理体制改革发展的经验，《密码法》明确了密码工作管理体制，包括两个方面的内容：一是国家、省、市、县四级密码工作管理体制，二是国家机关和涉及密码工作的单位的密码工作职责。

**19.问：四级密码工作管理体制的含义?**

答：《密码法》赋予了国家、省、市、县四级密码管理部门行政管理职责。

国家密码管理部门是指国家密码管理局。为更好地履行对全国的密码管理职能，2005年1月，中央机构编制委员会批准成立国家密码管理局。2008年3月，国家密码管理局列入国务院部委管理的国家局序列。2018年3月，《国务院关于部委管理的国家局设置的通知》(国发〔2018〕7号)明确规定，国家密码管理局与中央密码工作领导小组办公室，一个机构两块牌子，列入中共中央直属机关的下属机构序列。

国家密码管理局的主要职责是：组织贯彻落实党和国家关于密码工作的方针政策和法律法规，研究提出解决密码工作发展中重大问题的建议；拟订密码工作发展规划，起草密码工作法规并负责密码法规的解释，组织拟订密码相关标准；依法履行密码行政管理职能，管理密码科研、生产、装备(销售)、检测认证及使用，查处密码泄密事件和违法违规研制、使用密码行为，负责有关密码的涉外事宜；对密码工作机构实施业务领导；负责网络与信息系统中密码保障体系的规划和管理，规划、建设和管理国家密码基础设施；指导密码专业教育和密码学术交流，组织密码专业人才教育培训，对高等院校、科研机构、学术团体开展密码基础理论与应用技术研究、交流进行指导；承办中央密码工作领导小组的日常工作。

县级以上地方各级密码管理部门是指省(自治区、直辖市)、市(地、州、盟)、县(市、区、旗)密码管理局。为规范和加强密码管理部门的行政管理职能，《密码法》明确了国家、省、市、县四级分级负责的密码工作管理体制，赋予了国家、省、市、县四级密码管理部门行政管理职责，从体制机制上为密码管理部门依法履行密码管理职能提供了坚实的法治保障。

各级密码管理部门要认真贯彻落实《密码法》的明确要求，依法确立行政主体地位，全面履行《密码法》赋予的行政管理职能，加快建立权力清单、责任清单和负面清单，完善监督执法机制，规范执法方式，推动管理职能转变和管理方式创新，自觉做到“职权法定”、“权依法使”。

**20.问：国家机关和涉及密码工作的单位的密码工作职责是什么?**

答：国家机关和涉及密码工作的单位根据工作需要，承担相应的密码工作职责，是密码工作管理体制的重要组成部分。国家机关是指中央、省、市、县各级国家机关。涉及密码工作的单位是指除国家机关以外，承担密码管理职责的企事业单位等。这些机关、单位在其职责范围内负责本机关、本单位或本系统的密码工作。

**21.问：密码是如何分类的?**

答：《密码法》将密码分为核心密码、普通密码和商用密码，实行分类管理。核心密码用于保护国家绝密级、机密级、秘密级信息，普通密码用于保护国家机密级、秘密级信息，商用密码用于保护不属于国家秘密的信息。

**22.问：为什么要对密码实行分类管理?**

答：将密码分为核心密码、普通密码和商用密码，实行分类管理，是党中央确定的密码管理根本原则，是保障密码安全的基本策略，也是长期以来密码工作经验的科学总结。三类密码保护的对象不同，对其进行明确划分，有利于确保密码安全保密，有利于密码管理部门根据不同信息等级和使用对象，对密码实行科学管理，充分发挥三类密码在保护网络与信息安全中的核心支撑作用。对密码施行分类管理，也是国际通行做法。

**23.问：什么是核心密码、普通密码?**

答：核心密码、普通密码用于保护国家秘密信息，有力保障了中央政令军令安全，为维护国家网络空间主权、安全和发展利益构筑起密码屏障。按照《保守国家秘密法》的规定，国家秘密是指关系国家安全和利益，依照法定程序确定，在一定时间内只限一定范围的人员知悉的事项。《密码法》根据保护对象的不同，对核心密码、普通密码进行划分。核心密码用于保护国家绝密级、机密级、秘密级信息，普通密码用于保护国家机密级、秘密级信息。

**24.问：为什么要对核心密码、普通密码实行严格统一管理?**

答：密码管理部门按照中央要求，对核心密码、普通密码实行严格统一管理，针对核心密码、普通密码的科研、生产、服务、检测、装备、使用和销毁等各个环节制定了一系列严格的安全管理制度和保密措施，对核心密码、普通密码实行全生命周期的严格统一管理，明确了一系列保障措施。这是因为：第一，核心密码、普通密码用于保护国家秘密信息，直接关系国家安全和利益。第二，核心密码、普通密码本身也属于国家秘密，一旦泄密，将危害国家安全和利益。党政机关应当严格按照法律法规的有关规定使用核心密码、普通密码保护国家秘密信息，在法律范围内从事相关活动。第三，核心密码、普通密码的管理措施以及密码管理部门、密码工作机构及其工作人员开展核心密码、普通密码工作的保障措施等，需要通过国家立法提供法律依据，进一步提升密码工作的法治化保障水平。

**25.问：什么是商用密码?**

商用密码用于保护不属于国家秘密的信息。也就是说，商用密码可以用于保护除国家秘密之外的所有信息，既可以保护企业商业秘密、公民个人隐私，也可以保护政务领域中不属于国家秘密的工作信息。关于商用密码的名称，1996年，中央决定在我国大力发展商用密码，加强对商用密码的管理。1999年，国务院颁布施行《商用密码管理条例》(国务院令第273号)，商用密码的名称开始为社会所熟知和广泛使用。此后，中央文件和党内法规以及国家密码管理局制定发布的规范性文件均采用了“商用密码”这一名称。

**26.问：《密码法》在商用密码使用方面提出了什么样的管理要求?**

答：《密码法》规定公民、法人和其他组织可以依法使用商用密码保护网络与信息安全，对一般用户使用商用密码没有提出强制性要求。同时，为了保障关键信息基础设施安全稳定运行，维护国家安全和社会公共利益，《密码法》第二十七条规定了关键信息基础设施的商用密码使用要求。

公民、法人和其他组织可以依法使用商用密码，既是《密码法》赋予公民、法人和其他组织自主选择使用商用密码的权利，也是鼓励公民、法人和其他组织依法使用商用密码保护网络与信息安全。

**27.问：《密码法》为什么要鼓励和支持密码科学技术进步和创新?**

答：党的十九大报告指出，创新是引领发展的第一动力，是建设现代化经济体系的战略支撑。密码科学技术进步和创新是密码事业发展的灵魂，也是密码实现持续健康快速发展的动力源泉。紧紧牵住核心技术自主创新这个“牛鼻子”，牢牢掌握密码关键核心技术，是密码事业高质量发展的必由之路。坚持走中国特色密码自主创新道路，着眼密码科技前沿、立足网络空间安全、面向国家战略需求，加快创新驱动发展，是推进密码科技创新的基本要求。

**28.问：《密码法》在密码知识产权保护方面作了哪些具体规定?**

答：依法保护知识产权，对于激励科技创新，提高创新能力，促进创新成果合理分享，推动科技进步和经济社会发展，具有重要意义。

在密码工作实践中，无论是密码技术研究，还是密码检测认证、密码应用安全性评估、安全审查，都涉及密码知识产权保护。《密码法》在多个条款中对依法保护密码领域的知识产权作了具体规定。在商用密码检测认证方面，《密码法》对检测、认证机构在检测认证中所知悉的国家秘密、商业秘密和技术秘密的保密义务作了明确规定，并且规定了相应的法律责任。《密码法》还对密码管理部门和有关部门及其工作人员对在履行职责中知悉的商业秘密和个人隐私的保密义务作了明确规定，并且规定了相应的法律责任。

密码知识产权保护对国内外产品、服务以及内外资企业一视同仁、同等适用，对外商投资企业的知识产权实行同等保护。

**29.问：为什么要加强密码人才培养和队伍建设?**

答：人才是核心竞争力，密码事业的发展，归根结底要靠密码人才。密码人才队伍是一支特殊的队伍，承担着密码科研、密码管理、密码服务保障等重要任务，肩负着保障国家网络与信息安全的重要职责。随着网络与信息化的飞速发展和密码的广泛应用，密码人才需求呈现快速增长态势，密码专业人才培养和学科建设取得重要进展。目前，国内已有超过100所高校开设了密码学专业或者密码学相关课程，培育了大量的密码专业人才，涌现出一批具有国际知名度的优秀领军人才。将加强密码人才培养和队伍建设写进《密码法》也是贯彻落实相关中央文件和党内法规的明确要求，与《网络安全法》关于加强网络安全人才培养的规定也是衔接一致的。

**30.问：《密码法》规定了什么样的密码工作表彰奖励制度?**

答：为充分调动广大密码工作人员做好密码工作的积极性和创造性，推动密码工作创新发展，贯彻落实党和国家功勋荣誉表彰奖励制度要求，党和国家设立了全国密码工作先进集体和先进工作者、密码科学技术进步奖励等密码工作表彰奖励制度。《密码法》第九条规定：“对在密码工作中作出突出贡献的组织和个人，按照国家有关规定给予表彰和奖励。”将这一系列表彰奖励制度保留、固化下来。

**31.问：密码工作表彰奖励的对象有哪些?**

答：密码工作表彰奖励的对象主要是在服务党和国家工作大局中发挥重要作用以及在密码科技进步中作出重要贡献的密码管理部门、密码工作机构、商用密码从业单位和密码工作人员等。表彰奖励工作贯彻“尊重劳动、尊重知识、尊重人才、尊重创造”的方针，注重面向一线，注重工作实绩，遵循鼓励创新、促进发展、公平公正、严格把关的原则，坚持精神奖励与物质奖励相结合、以精神奖励为主，体现先进性、代表性和时代性。

**32.问：为什么要加强密码安全教育?**

答：密码安全事关国家安全，密码安全意识是国家安全意识的重要内容。密码安全教育是密码工作的重要组成部分，对密码工作高质量发展起着重要的导向和促进作用。做好密码安全教育工作，对于正确贯彻中央关于密码工作的方针政策，提高全民密码安全意识，引导全社会合规、正确、有效使用密码，确保密码使用优质高效、确保密码管理安全可靠，具有重要意义。

**33.问：如何加强密码安全教育?**

答：密码安全教育要与学习贯彻总体国家安全观紧密结合起来，以学习宣传贯彻《密码法》为重要抓手，面向不同人群，开展不同形式的密码安全教育，增强安全教育的针对性和实效性。

一是充分利用“全民国家安全教育日”“国家网络安全宣传周”等平台，深入开展《密码法》普及宣传活动，推动密码安全教育进社会、进课堂、进教材、进网络。

二是充分利用传统媒体和新兴媒体，充分发挥中国密码学会、商用密码领域的行业协会等社会团体和全国商用密码展览会、《密码学报》、全国密码技术竞赛等学术、产业交流平台的作用，创新宣传方式和手段，加大密码知识科普工作的力度，增强密码社会认知度和应用密码保护信息安全的意识。

三是各级教育主管部门和公务员主管部门将密码安全教育纳入国民教育体系和公务员教育培训体系，加强对大中小学生密码常识和密码安全意识的培养，加大对各级领导干部进行密码培训的力度，推动密码知识进校园，进党校(行政学院)、干部学院。

**34.问：为什么要把密码安全教育纳入国民教育体系和公务员教育培训体系?**

答：将密码安全教育纳入国民教育体系，在各阶段的教育过程中，开展密码常识、密码安全意识的教育，有利于提高全民密码安全意识，提高全社会自觉使用密码保护网络与信息安全、维护国家密码安全的意识。

在公务员培训中，密码安全教育主要是关于密码常识、密码安全意识和密码工作的教育，将密码安全教育纳入公务员教育培训体系，有利于公务员在履行职责过程中更好地贯彻总体国家安全观，提高密码安全意识与履职能力。

**35.问：《密码法》对密码工作规划和经费做了什么样的规定?**

答：为保障密码工作顺利开展，充分发挥密码在网络与信息安全中的基础支撑作用，《密码法》第十一条规定：“县级以上人民政府应当将密码工作纳入本级国民经济和社会发展规划，所需经费列入本级财政预算。”

**36.问：《密码法》对禁止利用密码从事违法犯罪活动做了什么样的规定?**

答：密码是一把“双刃剑”，既可以用于合法的信息保护，也可能被用来从事违法犯罪活动。密码一旦被用来从事违法犯罪活动，将严重危害国家安全、社会公共利益和公民个人合法权益。因此，《密码法》第十二条明确规定：“任何组织或者个人不得窃取他人加密保护的信息或者非法侵入他人的密码保障系统。任何组织或者个人不得利用密码从事危害国家安全、社会公共利益、他人合法权益等违法犯罪活动。”

**37.问：什么是“窃取他人加密保护的信息或者非法侵入他人的密码保障系统”?**

答：窃取他人加密保护的信息，是指未经他人授权，采用非法攻击密码等方式获取他人加密保护的信息的违法行为。

非法侵入他人的密码保障系统，是指未经他人授权，采用非法攻击密码等方式进入他人的密码保障系统。这里的“密码保障系统”，是指采用密码技术、产品或者服务集成建设的，实现加密保护、安全认证功能的系统。

**38.问：《密码法》为什么规定“任何组织和个人不得利用密码从事危害国家安全、社会公共利益、他人合法权益等违法犯罪活动”?**

答：随着网络信息技术的不断发展，利用密码从事违法犯罪活动的案例屡见不鲜，造成了广泛的社会影响。例如，2017年5月，一款名为“魔哭”(WannaCry)的蠕虫勒索软件袭击全球网络。它加密受害者电脑内的重要文件，除非受害者通过比特币交出赎金，否则加密文件无法恢复。“魔哭”勒索软件的影响范围覆盖全球150多个国家和地区，超过30万台设备受到感染和影响。我国有3万多家机构、数十万台设备受到该软件袭击，给国家、社会和公民个人财产造成巨大损失，严重危害了国家安全和社会稳定。

此外，《密码法》关于不得利用密码从事危害国家安全、社会公共利益、他人合法权益等违法犯罪活动的规定也是与《刑法》、《治安管理处罚法》、《网络安全法》等有关法律、行政法规的规定相衔接的。

**39.问：核心密码和普通密码遵循什么样的管理原则?**

答：核心密码、普通密码用于保护国家秘密信息，其本身也属于国家秘密，直接关系国家安全。

《密码法》从以下几个方面规定了核心密码、普通密码的管理原则。

一是国家加强核心密码、普通密码的科学规划、管理和使用。为深入贯彻落实党中央对密码工作的决策部署，国家着眼密码工作长远发展，加强核心密码、普通密码的科学规划、管理和使用，确保核心密码、普通密码安全。

二是加强制度建设，完善管理措施。国家密码管理部门和有关部门制定印发了核心密码、普通密码管理的一系列法规制度和标准规范，对核心密码、普通密码的科研、生产、服务、检测、装备、使用和销毁等各个环节实行全生命周期的严格统一管理。

三是增强密码安全保障能力。国家加强密码保障体系和密码安全监管能力建设，强化密码安全监测预警、安全风险评估、应急处置和监督管理等工作，夯实密码安全基础。

**40.问：《密码法》对核心密码、普通密码使用作了哪些规定?**

答：《密码法》第十四条明确规定：在有线、无线通信中传递的国家秘密信息，以及存储、处理国家秘密信息的信息系统，应当依照法律、行政法规和国家有关规定使用核心密码、普通密码进行加密保护、安全认证。

**41.问：密码工作机构需要承担哪些安全保密管理责任?**

答：《密码法》第十五条规定：从事核心密码、普通密码科研、生产、服务、检测、装备、使用和销毁等工作的机构(以下统称密码工作机构)，应当按照法律、行政法规、国家有关规定以及核心密码、普通密码标准的要求，建立健全安全管理制度，采取严格的保密措施和保密责任制，确保核心密码、普通密码的安全。

《密码法》中所称密码工作机构，是指从事核心密码、普通密码科研、生产、服务、检测、装备、使用和销毁等工作的机构。密码工作机构应当按照《密码法》和相关法律法规的要求，在科研、生产、服务、检测、装备、使用和销毁等各个环节建立健全安全管理制度，将保密措施和保密责任制规范化、制度化和体系化，有效保证核心密码、普通密码自身的安全，进而实现其所保护的国家秘密信息的安全。

**42.问：《密码法》对核心密码、普通密码工作的监督检查作了哪些规定?**

答：《密码法》第十六条规定：密码管理部门依法对密码工作机构的核心密码、普通密码工作进行指导、监督和检查，密码工作机构应当配合。

密码工作机构是密码管理部门的管理对象。密码管理部门按照《密码法》和其他有关法律法规的规定，对密码工作机构开展核心密码、普通密码工作的情况进行指导、监督和检查。主要内容是，密码工作机构是否严格依照法律、法规和国家有关规定开展核心密码、普通密码工作，正当行使权利和履行义务。《密码法》同时规定密码管理部门在行使上述监督检查职权时，必须以法律法规和有关政策为依据，不能随意扩大其职权。配合密码管理部门的指导、监督和检查，属于密码工作机构的法定义务，必须履行。

**43.问：为什么要建立核心密码、普通密码安全协作机制?**

答：《密码法》第十七条第一款规定：密码管理部门根据工作需要会同有关部门建立核心密码、普通密码的安全监测预警、安全风险评估、信息通报、重大事项会商和应急处置等协作机制，确保核心密码、普通密码安全管理的协同联动和有序高效。

为贯彻落实总体国家安全观，确保核心密码、普通密码安全，全天候全方位感知密码安全态势，就必须统筹协调国家有关部门共同推进密码安全管理工作，建立密码管理部门和有关部门间的监测预警、风险评估、信息通报、重大事项会商、应急处置等协作机制，准确把握密码安全风险发生的规律、动向、态势，实现密码情报信息的及时收集、准确分析、有效使用和共享，提高密码安全事件的应对处置能力。

**44.问：核心密码、普通密码安全协作机制具体包括哪些内容?**

答：《密码法》规定的密码管理部门会同有关部门建立的核心密码、普通密码安全协作机制主要包括安全监测预警、安全风险评估、信息通报、重大事项会商和应急处置等协作机制。

密码安全监测预警，是指针对包括窃取加密保护的信息，非法攻击、侵入密码保障系统等密码安全风险进行持续性监测，收集相关信息，发出预警信号，报告危险情况，最大程度降低密码安全事件造成的损害。

密码安全风险评估，是指对密码安全风险以及密码安全事件造成的影响进行科学的分析、研判和评估。

密码安全信息通报，是指密码管理部门和公安、国家安全、网信、工业和信息化、保密等有关部门相互通报密码安全风险以及密码安全事件等相关信息，通过整合多方资源、交流共享密码安全信息，实现密码安全的综合防控和主动防范。

密码安全重大事项会商，是指密码管理部门和公安、国家安全、网信、工业和信息化、保密等有关部门，共同研究、协商解决密码安全重大问题。

密码安全应急处置，是指通过制定应急预案、组织应急演练、开展应急响应等措施，将密码安全事件造成的危害后果和不利影响降低到最低限度。

**45.问：密码工作机构发现密码泄密等安全问题时如何处置?**

答：《密码法》第十七条第二款规定：密码工作机构发现核心密码、普通密码泄密或者影响核心密码、普通密码安全的重大问题、风险隐患的，应当立即采取应对措施，并及时向保密行政管理部门、密码管理部门报告，由保密行政管理部门、密码管理部门会同有关部门组织开展调查、处置，并指导有关密码工作机构及时消除安全隐患。

核心密码、普通密码属于国家秘密。密码工作具有很强的系统性，牵一发而动全身，凡是涉及密码安全的重大问题、风险隐患，都必须高度重视，及时进行处理，防止任何隐患演化为全局性问题和风险。

**46.问：核心密码、普通密码泄密主要指哪些情形?**

答：核心密码、普通密码泄密既包括核心密码、普通密码故意泄密，也包括核心密码、普通密码过失泄密，主要有以下三种情形：一是使核心密码、普通密码被不应知悉者知悉；二是使核心密码、普通密码超出了限定的接触范围，而不能证明未被不应知悉者知悉；三是核心密码、普通密码丢失，下落不明。

**47.问：影响核心密码、普通密码安全的重大问题、风险隐患是指什么?**

答：影响核心密码、普通密码安全的重大问题、风险隐患，是指核心密码、普通密码设备、部件、系统等发生损毁、中断、被攻击侵入等情况，已经或可能对密码安全构成威胁。

**48.问：出现密码安全问题时，密码工作机构要立即采取什么样的应对措施?**

答：采取应对措施是指为避免核心密码、普通密码泄密或减轻泄密后果而采取的一切合法和必要的措施。究竟如何采取应对措施以及采取何种应对措施，应根据当时的具体情况和现实条件作出决定。要求密码工作机构在发生核心密码、普通密码泄密等安全问题时及时报告，是为了让保密行政管理部门、密码管理部门及时了解情况，以便采取相应措施，及时组织查处，最大限度地减少可能造成的损害。

**49. 问：核心密码、普通密码泄密案件查处由哪些部门负责?**

答：为规范和加强密码泄密案件等安全问题查处工作，参照《保守国家秘密法》的规定，同时考虑到密码工作的特性和密码管理部门的管理实践，《密码法》规定，由保密行政管理部门、密码管理部门会同有关部门组织开展核心密码、普通密码泄密案件等安全问题的调查、处置工作。

**50.问：查处核心密码、普通密码泄密案件，主要包括哪些工作内容?**

答：核心密码、普通密码泄密案件查处的主要工作内容包括：一是查明核心密码、普通密码泄密事项的内容与密级，对于密码下落不明的，分析研判去向；二是查明案件事实、主要情节和有关责任人员；三是要求有关机关、单位及时采取必要的补救措施；四是根据有关法律法规和国家有关规定对责任人员提出处理建议，并督促机关、单位作出处理；五是针对案件暴露出的问题，指导有关密码工作机构及时消除安全隐患。

**51.问：《密码法》对核心密码、普通密码工作机构和人员管理作了哪些规定?**

答：《密码法》第十八条规定：国家加强密码工作机构建设，保障其履行工作职责。国家建立适应核心密码、普通密码工作需要的人员录用、选调、保密、考核、培训、待遇、奖惩、交流、退出等管理制度。

**52.问：为什么要加强核心密码、普通密码工作机构建设?**

答：密码工作机构承担着核心密码、普通密码的科研、生产、服务、检测、装备、使用和销毁等重要任务，肩负着保障国家网络与信息安全的重要职责，应当加强密码工作机构建设，在人力、物力、财力等方面加大保障力度，保障其有效履行工作职责。

**53.问：核心密码、普通密码工作人员要遵守哪些管理规定?**

答：核心密码、普通密码工作人员直接接触和掌握着国家秘密，岗位特殊、责任重大。加强对这些特殊工作人员的培养、使用和激励，对其进行更严格的管理，直接关系到我国密码事业的健康发展。

《密码法》将现行有关中央文件和党内法规中关于核心密码、普通密码工作人员管理的制度转化为法律规定，主要包括：(1)密码工作人员按照涉密程度实行分类管理。(2)密码工作人员应当具有良好的政治素质和品行，具有胜任密码工作岗位所要求的工作能力。(3)密码工作人员上岗应当经过密码教育培训，掌握密码知识技能，签订保密承诺书，严格遵守密码管理规章制度，不得以任何方式泄露国家秘密。(4)密码工作人员出境应当经有关部门批准。(5)密码工作人员离岗离职实行脱密期管理。

**54.问：《密码法》为什么规定对核心密码、普通密码有关物品和人员提供免检等便利?**

答：《密码法》第十九条规定：密码管理部门因工作需要，按照国家有关规定，可以提请公安、交通运输、海关等部门对核心密码、普通密码有关物品和人员提供免检等便利，有关部门应当予以协助。

密码管理部门在工作中，需要配发递送核心密码、普通密码。由于核心密码、普通密码属于国家秘密，应当严格控制接触和知悉范围，并按照有关规定严格做到密不离人，有关物品、人员进出国(边)境、限制区域、场所，或者乘坐火车、飞机、轮船等交通工具时，不宜对有关物品和人员进行检查，否则可能造成泄密，危害国家安全。

**55.问：密码管理部门提请有关部门对核心密码、普通密码有关物品和人员提供免检等便利，必须符合什么条件?**

答：根据《密码法》规定，提请免检必须符合以下条件：

一是必须基于密码工作需要。提请免检必须为开展密码工作所必需，如果提出免检的要求与密码工作无关，则不能适用这一规定。

二是必须按照国家有关规定向有关部门提请。这里的“国家有关规定”，是指法律、行政法规和国家有关规定中关于免检的规定，以及国家密码管理部门与国家有关部门关于免检的具体条件、提请的程序、免检的具体范围等方面的规定。这里的“有关部门”，是指公安、交通运输、海关等履行法定检查职责的部门。这里规定的“提请”是一个必经的程序，密码管理部门在要求对有关物品和人员免检时，在一般情况下应事先向有关部门提出予以协助的请求。在一些特别紧急来不及事先提出请求的情况下，密码管理部门应向有关部门说明情况，取得支持。

三是提请免检的对象限于核心密码、普通密码有关物品和人员。

符合上述条件，公安、交通运输、海关等有关部门应当予以协助。

**56.问：密码管理部门和密码工作机构为什么要对其工作人员进行监督和安全审查?**

答：《密码法》第二十条规定：密码管理部门和密码工作机构应当建立健全严格的监督和安全审查制度，对其工作人员遵守法律和纪律等情况进行监督，并依法采取必要措施，定期或者不定期组织开展安全审查。

对核心密码、普通密码工作人员进行监督和开展安全审查，是确保密码工作人员纯洁可靠的一项有效措施，也是涉密人员管理的通行做法。密码管理部门和密码工作机构的工作人员经常接触核心密码、普通密码，掌握着国家秘密，性质特殊、责任重大，应当对其遵守法律和纪律等情况进行监督，并依法采取必要措施，定期或者不定期组织开展安全审查。

**57.问：密码管理部门和密码工作机构应当如何对其工作人员开展监督和安全审查?**

答：《密码法》要求密码管理部门和密码工作机构建立健全严格的密码工作人员监督管理制度，明确密码工作人员的权利、岗位责任和要求，对密码工作人员遵纪守法和履行职责等情况开展经常性的监督检查。

密码管理部门和密码工作机构在录用、选调密码工作人员前，必须按照有关规定组织开展安全审查，同时定期或者不定期对在职的密码工作人员组织开展安全审查。审查内容主要包括本人的政治条件、个人品行、家庭社会关系等。对密码工作人员要按照先审后用的原则，严把资格审查和录用关，不符合条件者坚决不予录用；审查不合格的密码工作人员，应当及时调离密码工作岗位。

**58.问：为什么要对商用密码实施管理?**

答：虽然商用密码用于保护不属于国家秘密的信息，但商用密码可用于保护工作秘密、商业秘密、个人信息等，用途非常广泛，直接关系国家安全、社会公共利益以及公民、法人和其他组织的合法权益，应当依法进行管理。

首先，商用密码是国际公认的两用物项，对商用密码实施管理，是国际通行做法。同时，商用密码广泛用于金融、电子政务、通信、能源、交通等关键信息基础设施的网络和信息系统，应当对其实施必要监管，对商用密码的合规、正确、有效应用提出明确要求，保障关键信息基础设施的安全稳定运行，维护国家安全和社会公共利益。

**59.问：《密码法》在商用密码管理方面的立法思路主要有哪些?**

答：《密码法》在商用密码管理方面的立法思路主要有以下三个方面：

一是坚决贯彻落实“放管服”改革要求，充分体现非歧视和公平竞争原则，进一步削减行政许可数量，最大限度减少对市场活动的直接干预，切实降低制度性交易成本，更好地激发市场活力和社会创造力，增强商用密码产业发展动力。

二是以转变政府职能为核心，管理方式由重事前审批更多地转为事中事后监管，以市场主体需求为导向，重视发挥标准化和检测认证的支撑作用，进一步创新监管方式，提升监管效能。

三是对于关系国家安全和社会公共利益，又难以通过市场机制或者事中事后监管方式进行有效管理的少数事项，规定了必要的行政许可和管制措施，坚决守住安全底线。

**60.问：国家在鼓励商用密码技术的研究开发方面，采取了哪些举措，取得了哪些成绩?**

答：《密码法》明确规定：国家鼓励商用密码技术的研究开发、学术交流、成果转化和推广应用。

在鼓励商用密码技术研究开发方面，国家设立密码发展基金，面向社会公开申报研究课题，鼓励社会力量参与商用密码技术的研究开发。密码发展基金累计支持课题近200个，多个课题成果达到了国际先进或国内领先水平，有力促进了我国商用密码基础理论研究、技术转化和产业应用。

同时，国家密码管理局推荐社会各方面所开发的优秀商用密码科研科技成果申报国家科技进步奖和密码科技进步奖(省部级)，鼓励商用密码技术研究开发，激发创新活力。截至2019年12月，商用密码领域共获得国家科技进步奖一等奖1项、二等奖5项，省部级密码科技进步奖60余项。

**61.问：国家在鼓励商用密码技术学术交流方面，采取了哪些举措，取得了哪些成绩?**

答：在鼓励商用密码技术学术交流方面，中国密码学会等学术组织充分发挥平台作用，创建密码科普馆，举办科技展览，积极开展密码科普活动，出版50多种密码相关书籍刊物，大力普及密码知识，密码学术交流活动日益丰富。同时，全国商用密码展览会、中国密码学会年会、《密码学报》、全国密码技术竞赛等已成为我国密码学术研究和产业对接的高端平台。在努力提升全民密码科学文化素质的同时，一批密码学术研究领军人才、青年密码学家开始在国际舞台上崭露头角，为商用密码的可持续发展提供了可靠的人才保障。

中国密码学会等学术组织还积极开展国际密码学术交流活动，加强与国际密码协会等国际组织及相关企业的联系与交流。2012年，中国密码学会成功承办国际密码协会三大密码学术年会之——亚洲密码年会，来自欧美亚非洲等31个国家和地区的325位正式代表参会，参会人数创历年亚密会之最，极大地促进了国内密码学者与国际密码学者间的学习和交流。2012年以来，中国密码学会连续多年与美国信息技术产业理事会联合举办商用密码技术国际学术研讨会，极大地促进了国内外密码学界和产业界之间的沟通交流。

**62.问：国家在鼓励商用密码技术的成果转化方面，取得了什么样的成绩?**

答：商用密码科研成果主要包括商用密码算法、协议、密钥管理方案等，而成果转化活动是一个复杂过程，转化的最终目的是形成新技术、新工艺、新材料、新产品，乃至发展新产业。也就是说，要形成现实的生产力，只有这样，才能实现该科研成果的价值。

以商用密码算法为例，我国自主设计的SM4分组密码算法、祖冲之(ZUC)密码算法、SM2椭圆曲线公钥密码算法、SM3密码杂凑算法，以及SM9标识密码算法等已成为商用密码国家标准或行业标准，标志着我国商用密码算法体系已经基本形成。SM系列算法经过了多轮安全性分析评估，在设计、实现方面均有各自特点和优势，有力地支撑了商用密码产业化、规模化发展，得到了越来越广泛的认可和应用。

**63.问：我国商用密码技术的推广应用取得了哪些成绩?**

答：得益于商用密码技术研发和成果转化的有力支撑，商用密码的应用领域不断扩大，应用程度不断加深，应用认可度不断提升，在维护国家安全、促进经济社会发展、保护公民、法人和其他组织合法权益方面发挥着越来越重要的作用。我国金融信息系统、第二代居民身份证管理系统、国家电力信息系统、社会保障信息系统、全国中小学学籍管理等系统中，都应用商用密码技术构建了密码保障体系。同时，商用密码的广泛应用也对高质量商用密码技术、产品和服务提出了迫切需求，反过来极大促进了商用密码技术的研发交流和转化运用。

**64.问：我国要健全什么样的商用密码市场体系?**

答：《密码法》第二十一条明确规定：“国家健全统一、开放、竞争、有序的商用密码市场体系。”这不仅确立了我国商用密码市场体系的基本特征，也是我国商用密码市场体系建设的根本目标。

统一是指商用密码市场体系在全国范围内应该是统一的，必须打破条块分割、地区封锁，商用密码可以在行业、地区之间自由流通。

开放是指商用密码市场体系既要对内开放，允许商用密码从业单位和商用密码产品、服务在全国范围内自由地跨地区流动，又要对外开放，依法平等对待包括外商投资企业在内的商用密码从业单位，通过与国际市场广泛联系，积极参与国际分工与竞争。

竞争是指商用密码市场体系必须在一个公平竞争的环境下运行。只有通过充分竞争、优胜劣汰，形成合理正面的价格信号，才能有效引导商用密码的进步和流通，实现资源优化配置。

有序是指有一定的规则来维持商用密码市场的正常秩序，保证公平竞争和资源合理流动。这种规则既包括法律法规，也包括行业规范、国际惯例、商业信用等。

建立统一、开放、竞争、有序的商用密码市场体系，是市场经济所追求的“公平与效率”原则的体现，是促进商用密码持续发展的内在要求，也是商用密码国际化的题中之义。

**65.问：我国商用密码产业的基础怎么样?**

答：经过多年发展，我国商用密码产业取得长足进步，满足网络空间条件下差异化、多样化应用需求的能力不断提升，产业支撑能力显著增强。

首先，商用密码产业队伍持续壮大。截至2019年12月，商用密码从业单位已达1000多家。随着信息化发展对密码需求的不断增长，以商用密码为主业的上市公司越来越多，一批具有国际影响力的旗舰企业，踊跃进入商用密码产业领域，按照商用密码管理政策法规和标准规范研制商用密码产品、提供商用密码服务。这些企业活跃在商用密码产业链条的各个领域，形成了分布合理、竞争有序、创新力强的商用密码产业队伍，创造了巨大的经济效益和社会效益。

其次，商用密码产品种类不断丰富。截至2019年12月，通过国家密码管理局审批的商用密码通用产品有2000余款。2019年，全年共销售商用密码产品19亿台/套。从产品形态上，覆盖芯片、板卡、整机、系统等全产业链；从功能性能上，一批关键、基础、高性能商用密码产品推向市场，基本形成层次分明、功能完善、性能优异的产品体系；从应用领域上，更多满足电力、公安、交通、税务、金融等领域密码应用需求的产品可供选择，也有一批针对移动互联网、物联网、云计算、大数据等新兴领域的特定商用密码产品研制成功并得到应用。

此外，商用密码检测和电子认证服务能力进一步增强。密码检测基础理论、技术平台建设、运行机制等方面都取得新突破，多项成果达到国际先进水平，较好地满足了商用密码管理和产业发展对检测评估的需求。电子认证服务正在逐步构建一个以国家电子认证根CA为认证源点，辐射全国各地区各行业、连接上亿用户的电子认证体系。

**66.问：《密码法》在对待外商投资企业方面遵循什么样的管理原则?**

答：《密码法》第二十一条第二款规定：各级人民政府及其有关部门应当遵循非歧视原则，依法平等对待包括外商投资企业在内的商用密码科研、生产、销售、服务、进出口等单位(以下统称商用密码从业单位)。国家鼓励在外商投资过程中基于自愿原则和商业规则开展商用密码技术合作。行政机关及其工作人员不得利用行政手段强制转让商用密码技术。

《密码法》充分体现非歧视和公平竞争原则，按照“放管服”改革要求，进一步削减行政许可数量，发挥标准引领作用，加强检测认证体系建设，激发市场主体活力和社会创造力，有关许可和检测认证体系对国内外产品、服务以及内外资企业一视同仁、同等适用。

知识产权保护也是《密码法》突出强调的内容。《密码法》对商用密码技术合作的知识产权保护进行具体规定，明确商用密码技术合作的前提是基于自愿原则和商业规则，行政机关及其工作人员不得利用行政手段强制转让商用密码技术。

《密码法》一方面回应了各有关方面对我国外商投资过程中知识产权保护尤其是技术合作、转让的关切，澄清问题，消除疑虑；另一方面，也表明了我国不利用行政强制手段强制转让商用密码技术的态度，依法平等保护包括外商投资企业在内所有市场主体的商用密码知识产权，切实健全统一、开放、竞争、有序的商用密码市场体系。

**67.问：《密码法》关于商用密码标准体系的规定有哪些?**

答：《密码法》第二十二条规定：国家建立和完善商用密码标准体系。国务院标准化行政主管部门和国家密码管理部门依据各自职责，组织制定商用密码国家标准、行业标准。国家支持社会团体、企业利用自主创新技术制定高于国家标准、行业标准相关技术要求的商用密码团体标准、企业标准。

商用密码标准化是实现商用密码技术自主创新、促进商用密码产业发展、构建商用密码应用体系的重要支撑。《密码法》明确商用密码标准体系包括商用密码国家标准、行业标准、团体标准和企业标准。

商用密码国家标准、行业标准属于政府主导制定的标准，商用密码团体标准、企业标准属于市场主体自主制定的标准。其中，商用密码国家标准由国家标准化管理委员会组织制定，代号为GB。商用密码行业标准由国家密码管理局组织制定，报国家标准化管理委员会备案，代号为GM。商用密码团体标准由商用密码领域的学会、协会等社会团体制定，商用密码企业标准由商用密码企业制定或者企业联合制定。

**68.问：什么是密码行业标准化技术委员会，它的主要职责是什么?**

答：2011年10月，经国家标准化管理委员会批准，国家密码管理局设立了密码行业标准化技术委员会。密码行业标准化技术委员会作为我国密码行业唯一标准化组织，受国家密码管理局委托，主要职责包括：(1)提出密码行业标准规划和年度标准制定、修订计划的建议：(2)组织密码行业标准的编写、审查、复审等工作；(3)组织密码领域的国家和行业标准的宣传贯彻，推荐密码领域标准化成果申报科技进步奖励，或向国家标准化管理委员会提出项目奖励建议；(4)受国家标准化管理委员会委托，对相关国际标准文件进行表决、审查我国提案，并组织开展国际技术交流与合作等。

**69.问：当前商用密码行业标准分为哪几类?**

答：当前，商用密码的行业标准分为基础类标准、应用类标准、检测类标准和管理类标准。基础类标准为其他三类标准提供了底层、共性支撑(如术语、算法、协议、产品等)；检测类标准为基础类标准和应用类标准提供了合法性检测的功能，保障商用密码使用的合法性；管理类标准为其他三类标准提供了管理功能；应用类标准为上层具体的密码产品、服务应用提供支持。

**70.问：目前我国商用密码标准体系建设情况如何?**

答：截至2019年12月，国家标准化管理委员会已发布商用密码国家标准29项，国家密码管理局已发布商用密码行业标准91项，覆盖商用密码技术、产品、服务、应用、检测和管理等多个领域，构建了较为齐全完备的商用密码标准体系，有效发挥了商用密码标准在引领科技进步、推动产业发展、促进互联互通、助力应用推进、优化管理服务等方面的重要作用。

**71.问：我国商用密码国际标准化开展情况如何?**

答：《密码法》第二十三条第一款规定：国家推动参与商用密码国际标准化活动，参与制定商用密码国际标准，推进商用密码中国标准与国外标准之间的转化运用。

我国高度重视商用密码国际标准化工作，大力推进以我国自主设计研制的SM系列密码算法为代表的中国商用密码标准纳入国际标准，积极参与国际标准化活动，加强国际交流合作。2011年9月，我国设计的祖冲之(ZUC)算法纳入国际第三代合作伙伴计划组织(3GPP)的4G移动通信标准，用于移动通信系统空中传输信道的信息加密和完整性保护，这是我国密码算法首次成为国际标准。2015年5月起，我国陆续向ISO提出了将SM2、SM3、SM4和SM9算法纳入国际标准的提案。2017年，SM2和SM9算法正式成为ISO/IEC国际标准。2018年，SM3算法正式成为ISO/IEC国际标准。我国商用密码国际标准体系已初步成型，为密码在全球范围的发展与应用提供了中国方案，贡献了中国智慧。

在转化运用国际标准方面，商用密码行业标准GM/T0028《密码模块安全技术要求》和GM/T0039《密码模块安全检测要求》，分别参考国际标准ISO19790和ISO24759编制，为规范商用密码产品管理、提升商用密码产品安全防护能力发挥了重要作用，充分体现了商用密码标准制定的开放性。

**72.问：为什么要鼓励企业、社会团体和教育、科研机构等参与商用密码国际标准化活动?**

答：《密码法》第二十三条第二款规定：国家鼓励企业、社会团体和教育、科研机构等参与商用密码国际标准化活动。

企业、社会团体和教育、科研机构等全面深入地参与商用密码国际标准的制修订等国际标准化活动，是全球化的必然趋势和要求，有利于提升商用密码技术的全球影响力，同时也为降低包括密码脆弱性在内的全球网络安全整体风险贡献中国智慧和提供中国方案。

**73.问：商用密码标准具备什么样的法律效力?**

答：《密码法》第二十四条规定：商用密码从业单位开展商用密码活动，应当符合有关法律、行政法规、商用密码强制性国家标准以及该从业单位公开标准的技术要求。国家鼓励商用密码从业单位采用商用密码推荐性国家标准、行业标准，提升商用密码的防护能力，维护用户的合法权益。

商用密码从业单位开展商用密码活动应当依照有关法律、行政法规的规定行使权利和履行义务，是遵守法律的必然要求。商用密码从业单位开展商用密码活动，除了遵守法律、行政法规，还应当符合商用密码强制性国家标准以及该从业单位公开标准的技术要求。此外，国家鼓励商用密码从业单位采用商用密码推荐性国家标准、行业标准。

**74.问：什么是商用密码强制性国家标准和推荐性国家标准、行业标准?**

答：我国标准按照实施效力分为强制性标准和推荐性标准。强制性标准仅有国家标准一级。推荐性标准包括推荐性国家标准和行业标准。也就是说，商用密码行业标准都是推荐性标准。

强制性标准必须执行，不符合强制性标准的产品、服务，不得生产、销售、进口或者提供。违反强制性标准的，依法承担相应的法律责任。

国家鼓励采用推荐性标准，即从业单位自愿采用推荐性标准。同时国家还会采取一些正向激励措施，鼓励企业采用推荐性标准。但在有些情况下，推荐性标准的效力会发生转化，必须执行，例如：(1)推荐性标准被相关法律、法规、规章等引用，则该推荐性标准具有相应的强制约束力，应当按照法律、法规、规章的相关规定予以实施。(2)推荐性标准被企业进行了自我声明公开的，企业必须执行该推荐性标准。企业生产的产品与明示标准不一致的，根据《产品质量法》等法律法规承担相应的法律责任。(3)推荐性标准被合同双方作为产品或服务交付的质量依据的，该推荐性标准对合同双方具有约束力，双方必须执行该推荐性标准，并依据《合同法》的规定承担法律责任。

**75.问：什么是商用密码从业单位公开标准的技术要求，它有什么作用?**

答：《密码法》规定了企业标准自我声明公开和监督制度，调整的对象是企业生产的产品和提供的服务所执行的标准，这类标准规定了企业生产的产品和提供的服务所应达到的各类技术指标和要求，是企业对其产品和服务质量的硬承诺，应当公开并接受市场监督。

企业生产的商用密码产品和提供的商用密码服务，如果执行国家标准、行业标准和团体标准，企业应该公开相应的标准名称和标准编号；如果企业生产的产品和提供的服务所执行的标准是本企业制定的企业标准，企业除了公开相应的标准名称和标准编号，还应当公开企业产品、服务的技术指标。公开指标的类别和内容由企业根据自身特点自主确定，企业应对公开的产品和服务标准的真实性、准确性、合法性负责。

企业生产的产品和提供的服务应当符合企业自我声明公开标准提出的技术要求，不符合企业自我声明公开标准提出的技术要求的，应依法承担相应的责任。

**76.问：建设商用密码检测认证体系的意义是什么?**

答：商用密码检测认证是商用密码治理体系的重要基础，在商用密码市场准入、事中事后监管、应用推进等方面发挥着关键支撑作用：面向商用密码从业单位能够引导提质升级，增加市场有效供给；面向管理部门能够支持行政监管，提高市场监管效能；面向社会各方能够推动诚信建设，营造良好市场环境；面向国际市场能够促进规则对接，提升市场开放程度。

《密码法》第二十五条第一款明确提出推进商用密码检测认证体系建设，这是深化商用密码行政审批制度改革的重要内容，是依法管理商用密码、规范和促进商用密码应用、加强密码监管、增强商用密码安全保障能力的重要支撑。同时《密码法》第二十五条还明确了在商用密码检测认证中，自愿检测认证是主要方式。

**77.问：我国商用密码检测机构和认证机构现状如何?**

答：截至2019年12月，通过审批的商用密码产品检测机构共有3家，开展了智能密码钥匙、智能IC卡、POS密码应用系统、PCI-E密码卡、IPSecVPN安全网关、SSLVPN安全网关、安全认证网关、密码键盘、金融数据密码机、服务器密码机、签名验签服务器、时间戳服务器、安全门禁系统、动态令牌认证系统、安全电子签章系统、电子文件密码应用系统、可信计算类密码产品等的检测工作，完成了近2000款产品的密码检测、数百个信息系统的安全性评估。

目前，商用密码领域已有1家专门认证机构。与此同时，有关部门通过建立跨领域、跨行业的网络关键设备和网络安全专用产品、信息安全产品和密码应用系统密码检测认证机制，加强与金融、电力、通信、社保、交通等重点领域、行业的检测与认证技术交流，联合金融领域检测认证机构开展金融系统密码测评和认证，共同推动商用密码检测认证能力提升。

**78.问:商用密码检测、认证机构应取得什么资质?**

答:《密码法》第二十五条规定:商用密码检测、认证机构应当依法取得相关资质,并依照法律、行政法规的规定和商用密码检测认证技术规范、规则开展商用密码检测认证。

按照“放管服”改革要求,《密码法》将商用密码检测、认证机构资质纳入《认证认可条例》规定的认证认可制度体系中,由市场监管总局(国家认证认可监督管理委员会)会同国家密码管理局进行管理。商用密码检测、认证机构应当分别取得商用密码检测、认证机构资质。商用密码检测、认证机构依照《认证认可条例》等法律法规的规定和商用密码检测认证技术规范、规则开展检测认证活动。将商用密码检测认证制度纳入国家统一的检测认证制度体系,有利于增强商用密码检测认证制度的权威性、统一性。

**79.问:商用密码检测、认证机构是否应承担保密义务?**

答:在从事商用密码检测、认证活动的过程中,由于工作需要,商用密码检测、认证机构能够深入到所检测认证的商用密码产品、服务及其相关产品生产单位、服务提供单位中去,有可能接触到有关商业秘密乃至国家秘密。虽然商用密码检测、认证机构知悉国家秘密和商业秘密的途径是合法的,是在依法或依约定进行检测认证活动的过程中获取的,但是如果将这些秘密泄露给他人,就会损害国家安全和利益,或者损害商业秘密权利人的利益。因此,参照《认证认可条例》的规定,《密码法》第二十五条规定:商用密码检测、认证机构应当对其在商用密码检测认证中所知悉的国家秘密和商业秘密承担保密义务。

**80.问:商用密码产品的概念与范围是什么?**

答:商用密码产品,是指采用商用密码技术进行加密保护、安全认证的产品。商用密码产品可分为软件、芯片、模块、板卡、整机、系统六类。典型的商用密码产品包括:密码机,如链路密码机、网络密码机、服务器密码机、传真密码机、电话密码机等;密码芯片和模块,如第二代居民身份证、智能电卡、社会保障卡、金融芯片卡中使用的密码芯片、可信计算密码模块等。

**81.问:为什么要对特定商用密码产品实行强制性检测认证制度?**

答:《密码法》第二十六条规定:涉及国家安全、国计民生、社会公共利益的商用密码产品,应当依法列入网络关键设备和网络安全专用产品目录,由具备资格的机构检测认证合格后,方可销售或者提供。

对特定商用密码产品实行强制性检测认证,主要有三个方面的考虑:

一是该制度是维护国家安全和社会公共利益的需要。商用密码产品是一种专业技术性很强的特殊产品,广泛应用于国民经济和社会发展各领域,应用于关键信息基础设施,其质量与安全性直接关系国家安全和社会公共利益,需要通过检测认证的方式对其质量与安全性进行技术把关,规范商用密码产品市场准入。

二是该制度与《网络安全法》规定的网络关键设备和网络安全专用产品强制性检测认证制度衔接一致。涉及国家安全、国计民生、社会公共利益的商用密码产品作为网络关键设备和网络安全专用产品的一部分,依法列入网络关键设备和网络安全专用产品目录,由国家密码管理局会同国家互联网信息办公室、国家认证认可监督管理委员会等部门共同制定目录,共同认定检测、认证机构,共同开展检测认证。

三是强制性检测认证实施范围有限。强制性检测认证制度仅适用于涉及国家安全、国计民生、社会公共利益的商用密码产品,并通过制定产品目录明确界定管理范围,不会对市场和产业构成不必要的限制。

**82.问:商用密码产品检测认证避免重复检测认证的做法有哪些?**

答:为充分体现“放管服”改革精神，切实降低企业负担，节约检测认证资源,《密码法》第二十六条规定:商用密码产品检测认证适用《中华人民共和国网络安全法》的有关规定,避免重复检测认证。具体做法包括:一是制定并公布网络关键设备和网络安全专用产品目录,提高检测认证的透明度,避免适用检测认证制度的产品的重复。二是推动检测认证结果互认,减少某一类产品检测认证项目的重复。

**83.问:商用密码服务的概念与范围是什么?**

答:商用密码服务,是指基于商用密码专业技术、技能和设施,为他人提供集成、运营、监理等商用密码支持和保障的活动。典型的商用密码服务包括:密码保障系统集成(如数字证书认证系统集成),是指为他人集成建设实现密码功能的系统,保护他人网络与信息系统的安全。密码保障系统运营(如增值税发票防伪税控系统运营),是指为保证他人实现密码功能的系统的正常运行提供安全管理和维护。

**84.问:为什么要对使用网络关键设备和网络安全专用产品的商用密码服务实行强制性认证制度?**

答:《密码法》第二十六条规定:商用密码服务使用网络关键设备和网络安全专用产品的,应当经商用密码认证机构对该商用密码服务认证合格。

对使用网络关键设备和网络安全专用产品的商用密码服务实行强制性认证制度,主要有两个方面的考虑:一是该制度是维护国家安全和社会公共利益的需要。商用密码服务是一种专业技术性很强的特殊服务,广泛应用于国民经济和社会发展各领域,应用于关键信息基础设施,其质量与安全性直接关系国家安全和社会公共利益。由于密码功能实现的特殊性,网络关键设备和网络安全专用产品本身合格,并不意味着使用这些产品的商用密码服务就一定是安全的,需要通过认证的方式对其质量与安全性进行技术把关,规范商用密码服务市场准入。二是强制性认证实施范围有限。强制性认证制度仅适用于使用网络关键设备和网络安全专用产品的商用密码服务,并通过制定服务目录明确界定管理范围,不会对市场和产业构成不必要的限制。

**85.问:关键信息基础设施必须使用商用密码进行保护吗?**

答:《密码法》第二十七条规定: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。

《密码法》规定的关键信息基础设施商用密码使用要求是《网络安全法》规定的关键信息基础设施安全保护义务的重要组成部分。密码是保障网络与信息安全的核心技术和基础支撑。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,其运营者必须使用商用密码进行保护,而且使用的商用密码必须是合规、正确、有效的。

关键信息基础设施的运营者如果不使用或者不合规正确有效使用商用密码进行保护,将严重威胁关键信息基础设施的安全稳定运行,威胁国家安全和社会公共利益。因此,《密码法》对关键信息基础设施使用商用密码提出明确要求,有效保障关键信息基础设施安全。

**86.问：商用密码应用安全性评估的目的是什么?**

答:商用密码应用安全性评估,是指在采用商用密码技术、产品和服务集成建设的网络和信息系统中,对其密码应用的合规性、正确性和有效性进行评估。

建立完善商用密码应用安全性评估制度,对关键信息基础设施商用密码应用的合规性、正确性和有效性进行评估,对于有效规范密码应用,切实保障国家网络和信息安全,具有重要作用。

商用密码应用安全性评估同时也是网络安全等级保护和关键信息基础设施安全保护制度的重要内容和技术手段。关键信息基础设施的运营者作为关键信息基础设施网络安全保护和密码使用的第一责任人,《密码法》要求其履行相应的义务,按照相关法律法规和标准规范对关键信息基础设施密码应用的合规性、正确性、有效性和运维管理人员基本能力进行评估。

为有效控制安全风险,关键信息基础设施的运营者应当在规划、建设等必要阶段进行评估,系统投入运行后,还应当定期开展评估。

**87.问:商用密码应用安全性评估会造成重复评估、测评吗?**

答:为降低关键信息基础设施运营者负担,节约评估、测评资源,《密码法》第二十七条规定: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。商用密码应用安全性评估与关键信息基础设施网络安全检测评估、网络安全等级测评在内容上有所区分,在实施中统筹考虑、协调开展,相互衔接,避免重复评估、测评。

**88.问:为什么对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实行国家安全审查制度?**

答:《密码法》第二十七条规定: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。

对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实行国家安全审查制度,主要有以下考虑:一是该制度是维护国家安全和社会公共利益的需要,符合世贸组织规则,也是国际通行做法。国家安全审查可以防止关键信息基础设施因使用的产品和服务存在安全缺陷或隐患而受到攻击、破坏,或者存储的数据资源被窃取、泄露,从而提高关键信息基础设施安全可控水平,有效保障关键信息基础设施安全。二是该制度是《国家安全法》《网络安全法》中明确规定的制度,与《网络安全法》关于网络安全审查制度的规定衔接一致。本条中的“国家安全审查”是网络安全审查的一部分,安全审查由国家互联网信息办公室会同国家密码管理局等有关部门共同组织开展,不存在制度交叉和重复审查问题。

**89.问:《密码法》对商用密码进出口有哪些规定?**

答:《密码法》第二十八条规定:国务院商务主管部门、国家密码管理部门依法对涉及国家安全、社会公共利益且具有加密保护功能的商用密码实施进口许可,对涉及国家安全、社会公共利益或者中国承担国际义务的商用密码实施出口管制。商用密码进口许可清单和出口管制清单由国务院商务主管部门会同国家密码管理部门和海关总署制定并公布。

大众消费类产品所采用的商用密码不实行进口许可和出口管制制度。

**90.问:为什么要对商用密码实行进口许可和出口管制?**

答:对商用密码实行进口许可和出口管制主要有三个方面的考虑:

一是该制度是维护国家安全和社会公共利益的需要。商用密码是一把“双刃剑”,既可以用于合法的信息保护,也可能被用来从事违法犯罪活动,应当对其实行进口许可和出口管制,维护国家安全和社会公共利益。

二是该制度符合世贸组织规则,也是国际通行做法。商用密码是国际公认的两用物项,对其实行进口许可和出口管制,符合世贸组织“安全例外”原则和我国《对外贸易法》的规定,也是国际通行做法。

三是该制度实施范围有限。进口许可制度仅适用于涉及国家安全、社会公共利益且具有加密保护功能的商用密码,出口管制制度仅适用于涉及国家安全、社会公共利益或者中国承担国际义务的商用密码,对大众消费类产品所采用的商用密码不实行进口许可和出口管制,并通过制定清单明确界定管理范围,不会对贸易造成影响。

**91. 问:大众消费类产品所采用的商用密码是否实行进口许可和出口管制?**

答:《密码法》第二十八条规定:大众消费类产品所采用的商用密码不实行进口许可和出口管制制度。

大众消费类产品所采用的商用密码,是指社会公众可以不受限制地通过常规零售渠道购买、供个人使用、不能轻易改变密码功能的产品或技术。大众消费类产品所采用的商用密码对国家安全、社会公共利益带来的风险较小且可控,对大众消费类产品所采用的商用密码不实行进口许可和出口管制制度,可最大限度减少对贸易的影响。这既是国际社会的通行做法,也符合我国现有商用密码进出口管理实践。

**92.问:《密码法》中关于电子政务电子认证服务管理的规定是什么?**

答:《密码法》第二十九条规定:国家密码管理部门对采用商用密码技术从事电子政务电子认证服务的机构进行认定,会同有关部门负责政务活动中使用电子签名、数据电文的管理。

电子政务电子认证服务是一种专业技术性很强的特殊服务,直接服务于政务部门的政务活动,涉及范围广,敏感信息多,其质量与安全性直接关系国家安全和社会公共利益,应当采取行政许可的方式对服务机构的电子政务电子认证服务能力进行评估,加强对建设、运维、应用和服务等各环节的行政监管和技术把关,确保其质量与安全性。《密码法》基于维护国家安全和社会公共利益的需要,设立了电子政务电子认证服务机构认定制度。

**93.问:国家密码管理部门对政务活动中使用电子签名、数据电文的管理要求有哪些?**

答:《密码法》第二十九条规定:国家密码管理部门会同有关部门负责政务活动中使用电子签名、数据电文的管理。

《电子签名法》第三十五条也规定:“国务院或者国务院规定的部门可以依据本法制定政务活动和其他社会活动中使用电子签名、数据电文的具体办法。”目前,国家密码管理局依据该条的规定管理政务活动中电子签名、数据电文的使用,制定的GM/T0014—2012《数字证书认证系统密码协议规范》、GM/T0047—2016《安全电子签章密码检测规范》、GM/T0044.2—2016《SM9标识密码算法第2部分:数字签名算法》、GM/T0031—2014《安全电子签章密码应用技术规范》等商用密码行业标准,对使用电子签名、数字电文提出了管理要求。

**94.问:《密码法》对商用密码领域的行业协会等组织作出了哪些规定?**

答:《密码法》第三十条规定:商用密码领域的行业协会等组织依照法律、行政法规及其章程的规定,为商用密码从业单位提供信息、技术、培训等服务,引导和督促商用密码从业单位依法开展商用密码活动,加强行业自律,推动行业诚信建设,促进行业健康发展。

**95.问:建立发展商用密码领域的行业协会等组织有什么意义?**

答:《密码法》结合商用密码发展实际,深化商用密码领域“放管服”改革,构建起现代化商用密码治理体系。商用密码治理体系作为一个有机整体,除了各有关管理部门要加强服务和管理外,还需要从业单位、社会组织、公民等各方面共同努力,参与商用密码社会共治。行业协会等组织作为介于密码管理部门和商用密码从业单位之间的社会组织,既是沟通管理部门和从业单位的桥梁与纽带,又是社会多元利益的协调机构,也是实现行业自律、规范行业行为、开展行业服务、保障公平竞争的社会组织,在社会管理、行业治理、行业自律中发挥了重要作用,既大大减少了政府的管理成本,又促进了行业自身的发展,显示了巨大的社会效益。

**96.问:商用密码领域的行业协会等组织的宗旨是什么?**

答:商用密码行业协会等组织代表本行业从业单位的利益,切实为从业单位服务。商用密码行业协会等组织根据授权进行行业统计,掌握国内外行业发展动态,收集、发布行业信息;依照有关规定创办刊物和网站,开展法律、政策、技术、管理、市场等咨询服务;参与行业资质认证、新技术和新产品鉴定及推广等相关工作;组织人才、技术、管理、法规等培训,帮助会员企业提高素质、增强创新能力、改善经营管理;受管理部门委托承办或根据市场和行业发展需要举办交易会、展览会等,为企业开拓市场创造条件。

**97.问:商用密码领域的行业协会等组织如何发挥桥梁纽带作用?**

答:通过积极向密码管理部门反映行业、会员诉求,提出商用密码行业发展和立法等方面的意见和建议,积极参与相关法律法规、宏观调控和产业政策的研究、制定,参与制定修订商用密码国家标准、行业标准和行业发展规划、行业准入条件,完善行业管理,促进行业发展。

**98.问:目前我国商用密码领域的行业协会等组织发展情况如何?**

答:随着我国商用密码的快速发展,商用密码领域的行业协会等组织也在不断发展壮大。截至2019年12月,北京、天津、上海、江苏、福建、江西、山东、广东、重庆、四川、陕西、深圳等地已经成立了区域性商用密码行业协会。此外,全国性和一些地方性商用密码领域的行业协会等组织也在抓紧建立。这些组织在服务商用密码从业单位、加强行业自律、推动诚信建设、促进产业发展方面发挥了重要的作用。

**99.问:商用密码行业协会等组织的行业自律职能主要是什么?**

答:行业自律是商用密码从业单位为维护共同利益、促进共同发展而开展的订立行业规范、规范行业行为、协调利益关系、维护公平竞争的自我管理、自我约束行为。商用密码行业自律的主要内容是围绕规范商用密码市场秩序,健全各项自律性管理制度,制定并组织实施行业职业道德准则,大力推动行业诚信建设,建立完善行业自律性管理约束机制,规范会员行为,协调会员关系,维护公平竞争的市场环境。

**100.问:《密码法》关于商用密码事中事后监管制度的要求是什么?**

答:《密码法》第三十一条规定:密码管理部门和有关部门建立日常监管和随机抽查相结合的商用密码事中事后监管制度。

《密码法》在商用密码领域深化“放管服”改革,坚持放管结合,在取消一批商用密码行政许可事项的基础上,把更多行政资源从事前审批转到事中事后监管上来,着力构建权责明确、公平公正、公开透明、简约高效的商用密码事中事后监管体系,确保监管“不缺位、不错位、不越位”。

商用密码事中事后监管的实施主体,是密码管理部门和其他涉及商用密码监督管理的有关部门,主要包括市场监管、网信、商务、海关等部门。密码管理部门和有关部门依法开展商用密码事中事后监管,对涉及多个部门的商用密码监管事项,主责部门发挥牵头作用,相关部门协同配合。

**101.问:商用密码事中事后监管如何开展?**

答:商用密码事中事后监管以日常检查为主、专项整治为辅,日常监管又以随机抽查为主。商用密码日常监管全面实行随机抽取检查对象、随机选派执法检查人员、抽查情况及查处结果及时向社会公开,原则上所有日常行政检查都通过“双随机、一公开”的方式进行。下一步,密码管理部门和有关部门将不断完善商用密码随机抽查相关配套制度和工作机制,健全跨部门联合抽查机制,避免对同一商用密码市场主体多头、重复检查。将随机抽查的比例频次、被抽查概率与抽查对象的信用等级、风险程度挂钩,对有不良信用记录、风险高的加大抽查力度,对信用较好、风险较低的适当减少抽查。抽查结果分别通过国家企业信用信息公示系统、“信用中国”网站、国家“互联网+监管”系统等进行公示。

商用密码事中事后监管的重要手段是深入推进“互联网+监管”,依托国家“互联网+监管”系统,建设统一的商用密码监督管理信息平台。加强商用密码监管信息归集共享,将各类商用密码相关的行政检查、行政处罚、行政强制等信息以及司法判决、违法失信、抽查抽检等信息进行关联整合,并归集到相关商用密码市场主体名下。充分运用大数据等技术,加强对风险的跟踪预警。提升商用密码事中事后监管的精准化、智能化水平。

**102.问:商用密码事中事后监管如何与社会信用体系相衔接?**

答:推进商用密码事中事后监管与社会信用体系相衔接,提升商用密码信用监管效能。以国家统一社会信用代码为标识,依法依规建立权威、统一、可查询的商用密码市场主体信用记录。大力推行商用密码从业单位及有关市场主体信用承诺制度,将信用承诺履行情况纳入信用记录。推进信用分级分类监管,依据商用密码从业单位信用情况,在监管方式、抽查比例和频次等方面采取差异化措施。规范认定并设立商用密码市场主体信用“黑名单”,强化失信联合惩戒,对失信主体在行业准入、获得信贷、出口退税、高消费等方面依法予以限制。建立健全信用修复、异议申诉等机制。在保护涉及国家秘密、商业秘密和个人隐私等信息的前提下,依法做好商用密码有关信用信息的公开工作。

**103.问:如何强化商用密码从业单位自律和社会监督?**

答:强化商用密码从业单位自律和社会监督,就是要充分调动社会各方力量参与商用密码监督管理,统筹社会各种资源支持商用密码社会治理,形成市场自律、社会监督和政府监管互为支撑的商用密码协同监管格局,切实管出公平、管出效率、管出活力,提高商用密码市场主体竞争力和市场效率,推动商用密码产业持续健康发展。

**104.问:《密码法》对密码管理部门和有关部门及其工作人员提出了什么样的保密要求?**

答:《密码法》第三十一条规定:密码管理部门和有关部门及其工作人员不得要求商用密码从业单位和商用密码检测、认证机构向其披露源代码等密码相关专有信息,并对其在履行职责中知悉的商业秘密和个人隐私严格保密,不得泄露或者非法向他人提供。

**105.问:《密码法》为什么要对密码管理部门和有关部门及其工作人员提出保密要求?**

答:密码管理部门和有关部门及其工作人员对在履行职责中知悉的商业秘密和个人隐私予以严格保密,是其基本的法定义务,也体现了行政机关对自身履职的严格要求。

密码管理部门和有关部门在依法履行职责的过程中会合理知悉有关商业秘密和个人隐私,虽然其知悉途径是合法的,但是如果将这些信息泄露给他人,就会损害商业秘密权利人的利益,或者损害公民个人的合法权益。为保护当事人合法权益,并保证密码管理活动的正常进行,密码管理部门和有关部门及其工作人员必须对在履行职责中知悉的商业秘密和个人隐私严格保密,不得泄露或者非法向他人提供。同时,《密码法》关于源代码等密码相关专有信息保护的规定是商用密码知识产权保护原则的又一具体措施。

**106.问:《密码法》对窃取他人加密保护的信息,非法侵入他人的密码保障系统,或者利用密码从事危害国家安全、社会公共利益、他人合法权益等违法活动,规定了什么样的法律责任?**

答:《密码法》第三十二条规定:违反本法第十二条规定,窃取他人加密保护的信息,非法侵入他人的密码保障系统,或者利用密码从事危害国家安全、社会公共利益、他人合法权益等违法活动的,由有关部门依照《中华人民共和国网络安全法》和其他有关法律、行政法规的规定追究法律责任。

《密码法》明确的从事密码违法活动具体包括三种情形:一是窃取他人加密保护的信息。二是非法侵入他人的密码保障系统。三是利用密码从事危害国家安全、社会公共利益、他人合法权益等违法活动。

**107.问:《密码法》明确哪些未按照要求使用核心密码、普通密码的情形?**

答:《密码法》明确了违反核心密码、普通密码使用要求的两种情形:一是在有线、无线通信中传递的国家秘密信息,以及存储、处理国家秘密信息的信息系统,未使用核心密码、普通密码进行加密保护、安全认证。二是在有线、无线通信中传递的国家秘密信息,以及存储、处理国家秘密信息的信息系统,虽然使用了核心密码、普通密码,但未能依照法律、行政法规和国家有关规定,合规、正确、有效地使用核心密码、普通密码进行加密保护、安全认证。

**108.问:《密码法》对未按照要求使用核心密码、普通密码的行为,规定了什么样的法律责任?**

答:《密码法》第三十三条规定:违反本法第十四条规定,未按照要求使用核心密码、普通密码的,由密码管理部门责令改正或者停止违法行为,给予警告;情节严重的,由密码管理部门建议有关国家机关、单位对直接负责的主管人员和其他直接责任人员依法给予处分或者处理。

此条规定的法律责任包括:

1.责令改正。所谓责令改正,是指有关主管部门依法要求违法行为人将其违法行为恢复到合法状态。

2.责令停止违法行为。所谓责令停止违法行为,是指有关主管部门依法要求违法行为人停止其实施的违法行为。

3.警告。所谓警告,是指有关主管部门对违法行为人进行训诫,使其认识到其行为的违法性。

4.处分。分为行政处分和党纪处分两种。本条中的“直接负责的主管人员”,是指在机关、单位实施的违法行为中起决定、批准、授意、指挥等作用的人员,一般是本机关、单位分管某一方面工作的负责人。“其他直接责任人员”,是指具体实施违法行为并起较大作用的人员,可以是机关、单位的管理人员、工作人员。

5.处理。所谓处理,是指对实施了相关违法行为,但不适用处分的人员,由有关主管部门依照有关法律、法规的规定作出的惩戒。这里所说的不适用处分的人员,主要是指在国家机关工作但不具有编制的聘任人员和企事业单位聘任的人员。

密码管理部门应当及时建议督促有关机关、单位对违法人员依法给予处分或者处理。

**109.问:《密码法》明确哪些核心密码、普通密码泄密等安全问题的情形?**

答:《密码法》明确了核心密码、普通密码泄密案件或者密码工作机构违反相关安全要求的具体情形:一是发生核心密码、普通密码泄密案件。二是发现核心密码、普通密码泄密或者影响核心密码、普通密码安全的重大问题、风险隐患,未立即采取应对措施。三是发现核心密码、普通密码泄密或者影响核心密码、普通密码安全的重大问题、风险隐患,未及时向保密行政管理部门、密码管理部门报告。

**110.问:《密码法》明确的核心密码、普通密码泄密等安全问题的法律责任具体包括哪些?**

答:《密码法》第三十四条规定:违反本法规定,发生核心密码、普通密码泄密案件的,由保密行政管理部门、密码管理部门建议有关国家机关、单位对直接负责的主管人员和其他直接责任人员依法给予处分或者处理。违反本法第十七条第二款规定,发现核心密码、普通密码泄密或者影响核心密码、普通密码安全的重大问题、风险隐患,未立即采取应对措施,或者未及时报告的,由保密行政管理部门、密码管理部门建议有关国家机关、单位对直接负责的主管人员和其他直接责任人员依法给予处分或者处理。

此条规定的法律责任包括:

1.处分。处分分为行政处分和党纪处分两种。本条中的“直接负责的主管人员”,是指在机关、单位实施的违法行为中起决定、批准、授意、指挥等作用的人员,一般是本机关、单位分管某一方面工作的负责人。“其他直接责任人员”,是指具体实施违法行为并起较大作用的人员,可以是机关、单位的管理人员、工作人员。

2.处理。所谓处理,是指对实施了相关违法行为,但不适用处分的人员,由有关主管部门依照有关法律、法规的规定作出的惩戒。这里所说的不适用处分的人员,主要是指在国家机关工作但不具有编制的聘任人员和企事业单位聘任的人员。

保密行政管理部门、密码管理部门应当及时建议督促有关机关、单位对违法人员依法给予处分或者处理。

**111.问:《密码法》对商用密码检测、认证机构违法规定了什么样的法律责任?**

答:《密码法》第三十五条规定:商用密码检测、认证机构违反本法第二十五条第二款、第三款规定开展商用密码检测认证的,由市场监督管理部门会同密码管理部门责令改正或者停止违法行为,给予警告,没收违法所得;违法所得三十万元以上的,可以并处违法所得一倍以上三倍以下罚款;没有违法所得或者违法所得不足三十万元的,可以并处十万元以上三十万元以下罚款;情节严重的,依法吊销相关资质。

此条规定的法律责任包括:

1.责令改正。所谓责令改正,是指有关主管部门依法要求违法行为人将其违法行为恢复到合法状态。

2.责令停止违法行为。所谓责令停止违法行为,是指有关主管部门依法要求违法行为人停止其实施的违法行为。

3.警告。所谓警告,是指有关主管部门对违法行为人进行训诫,使其认识到其行为的违法性。

4.没收违法所得。所谓没收违法所得,是指有关主管部门依法将违法行为人从事非法经营等获得的利益收归国有。

5.罚款。所谓罚款,是指有关主管部门依法强制违法行为人在一定期限内向国家缴纳一定数额的金钱。对于违法所得三十万元以上的,可以并处违法所得一倍以上三倍以下罚款;没有违法所得或者违法所得不足三十万元的,可以并处十万元以上三十万元以下罚款。

6.吊销相关资质。所谓吊销相关资质,是指有关主管部门依法收回违法行为人已经获得的从事某种活动的资格和权利。这里的相关资质,是指商用密码检测、认证机构资质。

**112.问:《密码法》明确什么情形属于违反商用密码产品、服务市场准入制度?**

答:《密码法》明确了违反商用密码产品、服务市场准入制度的两种情形:一是销售或者提供列入网络关键设备和网络安全专用产品目录的商用密码产品,未经具备资格的机构检测认证或者检测认证不合格。二是提供使用网络关键设备和网络安全专用产品的商用密码服务,未经商用密码认证机构认证或者认证不合格。本条规定的执法部门是市场监督管理部门会同密码管理部门。

**113.问:《密码法》对商用密码产品、服务市场准入违法规定了什么样的法律责任?**

答:《密码法》第三十六条规定:违反本法第二十六条规定,销售或者提供未经检测认证或者检测认证不合格的商用密码产品,或者提供未经认证或者认证不合格的商用密码服务的,由市场监督管理部门会同密码管理部门责令改正或者停止违法行为,给予警告,没收违法产品和违法所得;违法所得十万元以上的,可以并处违法所得一倍以上三倍以下罚款;没有违法所得或者违法所得不足十万元的,可以并处三万元以上十万元以下罚款。

此条规定的法律责任包括:

1.责令改正。所谓责令改正,是指有关主管部门依法要求违法行为人将其违法行为恢复到合法状态。

2.责令停止违法行为。所谓责令停止违法行为,是指有关主管部门依法要求违法行为人停止其实施的违法行为。

3.警告。所谓警告,是指有关主管部门对违法行为人进行训诫,使其认识到其行为的违法性。

4.没收违法产品和违法所得。所谓没收违法产品,是指没收违法销售、提供的产品以及违法提供的服务中使用的产品,包括尚未销售、提供和尚未使用的产品,以防止这些产品销售、提供或使用后,给使用者造成财产损失,危害国家安全和社会公共利益。所谓没收违法所得,是指有关主管部门依法将违法行为人从事非法经营等获得的利益收归国有。

5.罚款。所谓罚款,是指有关主管部门依法强制违法行为人在一定期限内向国家缴纳一定数额的金钱。对于违法所得十万元以上的,可以并处违法所得一倍以上三倍以下罚款;没有违法所得或者违法所得不足十万元的,可以并处三万元以上十万元以下罚款。

**114.问:《密码法》明确关键信息基础设施的运营者违反商用密码使用要求的情形有哪些?**

答:《密码法》明确了关键信息基础设施的运营者违反商用密码使用要求的具体情形:一是关键信息基础设施的运营者未按照要求使用商用密码。二是关键信息基础设施的运营者未按照要求开展商用密码应用安全性评估。三是关键信息基础设施的运营者使用未经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或者国家安全审查未通过的涉及商用密码的网络产品或者服务。

**115.问:《密码法》对关键信息基础设施的运营者未按照要求使用商用密码,或者未按照要求开展商用密码应用安全性评估,规定了哪些法律责任?**

答:《密码法》第三十七条规定:关键信息基础设施的运营者违反本法第二十七条第一款规定,未按照要求使用商用密码,或者未按照要求开展商用密码应用安全性评估的,由密码管理部门责令改正,给予警告;拒不改正或者导致危害网络安全等后果的,处十万元以上一百万元以下罚款,对直接负责的主管人员处一万元以上十万元以下罚款。

此条规定的法律责任包括:

1.责令改正。所谓责令改正,是指有关主管部门依法要求违法行为人将其违法行为恢复到合法状态。

2.警告。所谓警告,是指有关主管部门对违法行为人进行训诫,使其认识到其行为的违法性。

3.罚款。所谓罚款,是指有关主管部门依法强制违法行为人在一定期限内向国家缴纳一定数额的金钱。对于关键信息基础设施的运营者拒不改正或者导致危害网络安全等后果的,对关键信息基础设施的运营者处十万元以上一百万元以下罚款,对直接负责的主管人员处一万元以上十万元以下罚款。

**116.问:《密码法》对关键信息基础设施的运营者使用未经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或者国家安全审查未通过的涉及商用密码的网络产品或者服务,规定了哪些法律责任?**

答:《密码法》第三十七条第二款规定:关键信息基础设施的运营者违反本法第二十七条第二款规定,使用未经安全审查或者安全审查未通过的产品或者服务的,由有关主管部门责令停止使用,处采购金额一倍以上十倍以下罚款;对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款。

此条规定的法律责任包括:

1.责令停止使用。所谓责令停止使用,是指有关主管部门依法要求违法行为人停止使用未经安全审查或者安全审查未通过的产品或者服务。

2.罚款。所谓罚款,是指有关主管部门依法强制违法行为人在一定期限内向国家缴纳一定数额的金钱。对于关键信息基础设施的运营者违法使用未经安全审查或者安全审查未通过的产品或者服务的,处采购金额一倍以上十倍以下罚款;对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款。

**117.问:《密码法》对商用密码进出口违法的法律责任做了什么样的规定?**

答:《密码法》第三十八条规定:违反本法第二十八条实施进口许可、出口管制的规定,进出口商用密码的,由国务院商务主管部门或者海关依法予以处罚。

《密码法》明确了违反商用密码进口许可和出口管制制度的两种情形:一是未经许可,进口涉及国家安全、社会公共利益且具有加密保护功能的商用密码。二是未经许可,出口涉及国家安全、社会公共利益或者中国承担国际义务的商用密码。本条规定的执法部门是国务院商务主管部门或者海关,执法依据是《密码法》《对外贸易法》等法律、行政法规的规定。

**118.问:《密码法》对未经认定从事电子政务电子认证服务的行为,规定了什么样的法律责任?**

答:《密码法》第三十九条规定:违反本法第二十九条规定,未经认定从事电子政务电子认证服务的,由密码管理部门责令改正或者停止违法行为,给予警告,没收违法产品和违法所得;违法所得三十万元以上的,可以并处违法所得一倍以上三倍以下罚款;没有违法所得或者违法所得不足三十万元的,可以并处十万元以上三十万元以下罚款。

此条规定的法律责任包括:

1.责令改正。所谓责令改正,是指有关主管部门依法要求违法行为人将其违法行为恢复到合法状态。

2.责令停止违法行为。所谓责令停止违法行为,是指有关主管部门依法要求违法行为人停止其实施的违法行为。

3.警告。所谓警告,是指有关主管部门对违法行为人进行训诫,使其认识到其行为的违法性。

4.没收违法产品和违法所得。所谓没收违法产品,是指没收违法提供的、不符合强制性标准和要求的产品,包括尚未提供的产品,以防止这些产品提供后,给使用者造成财产损失,危害国家安全和社会公共利益。所谓没收违法所得,是指有关主管部门依法将违法行为人从事非法经营等获得的利益收归国有。

5.罚款。所谓罚款,是指有关主管部门依法强制违法行为人在一定期限内向国家缴纳一定数额的金钱。

**119.问:《密码法》对密码管理部门和有关部门、单位的工作人员在密码工作中违法的法律责任做了什么样的规定?**

答:《密码法》第四十条规定:密码管理部门和有关部门、单位的工作人员在密码工作中滥用职权、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和个人隐私的,依法给予处分。

《密码法》赋予了密码管理部门和有关部门、单位的工作人员的密码管理职责。本法第三十一条规定了密码管理部门和有关部门及其工作人员对在履行职责中知悉的商业秘密和个人隐私的保密义务。本条是对密码管理部门和有关部门、单位的工作人员违法的法律责任,具体包括:一是密码管理部门和有关部门、单位的工作人员在密码工作中滥用职权、玩忽职守、徇私舞弊。密码管理部门和有关部门、单位的工作人员应当依照《密码法》和其他行政法规规定的权限、程序等履行职责,不得怠于履行或者超越法定权限履行职责。二是密码管理部门和有关部门、单位的工作人员泄露、非法向他人提供在履行职责中知悉的商业秘密和个人隐私。

本条规定的法律责任是处分。处分分为行政处分和党纪处分两种。

**120.问:《密码法》对违反本法行为的刑事责任和民事责任做了什么样的衔接性规定?**

答:《密码法》第四十一条规定:违反本法规定,构成犯罪的,依法追究刑事责任;给他人造成损害的,依法承担民事责任。

法律责任分为民事责任、行政责任和刑事责任三类。同一违法行为,依法可能同时应承担民事责任、行政责任和刑事责任。《密码法》第三十二条至第四十条对违反本法规定应当承担的行政责任作了具体规定,本条对违反本法规定应当承担的民事责任和刑事责任作了衔接性规定。

**121.问:《密码法》关于密码管理规章制定权做了什么样的规定?**

答:《密码法》第四十二条规定:国家密码管理部门依照法律、行政法规的规定,制定密码管理规章。

本条明确了国家密码管理部门的规章制定权。《密码法》是密码工作的基本法律,针对密码和网络信息技术发展日新月异的突出特点,《密码法》中对密码管理制度只作了原则性规定。《密码法》出台后,国家密码管理局需要依照《密码法》等相关法律、行政法规,针对密码生产、销售、服务、进出口、检测认证等环节,制定公布一系列密码管理规章,及时补充、细化法律、行政法规的相关规定,增强密码法律法规的可操作性。

**122.问:国家密码管理部门将建立什么样的密码法律制度体系?**

答:《密码法》颁布实施后,国家密码管理局将深入贯彻落实党中央全面依法治国基本方略,在国家安全法治建设的总体框架下进一步推进密码法律制度体系建设,加强顶层设计和整体规划,按照党管密码、科学立法、民主立法的原则,统筹推进《商用密码管理条例》等配套行政法规、规章的制修订工作,及时制定出台一系列与《密码法》相互协调和衔接的规章,确保密码法规规章符合《密码法》确定的立法原则和基本制度,全方位扎紧织密法律制度的笼子,建立一个以《密码法》为核心,以《商用密码管理条例》等行政法规为基础,以核心密码、普通密码、商用密码等方面的规章和规范性文件为分支,权责明确、功能互补、协调一致的密码法律制度体系。

**123.问:《密码法》对于解放军和武警部队密码立法做了什么样的规定?**

答:《密码法》第四十三条规定:中国人民解放军和中国人民武装警察部队的密码工作管理办法,由中央军事委员会根据本法制定。

中央军事委员会是国家的最高军事机关,按照《立法法》规定,中央军事委员会根据宪法和法律制定军事法规。

中国人民解放军和中国人民武装警察部队的密码工作作为密码工作的重要组成部分,有其自身的特点和规律,法律规定由中央军事委员会根据本法的基本精神,结合解放军和武警部队自身实际,对解放军和武警部队的密码工作作出全面、系统的规定。

**124.问:《密码法》从何时开始施行?**

答:《密码法》第四十四条规定:本法自2020年1月1日起施行。

法律的施行日期,即法律的生效日期,是一部法律的重要组成部分。《立法法》第五十七条规定,法律应当明确规定施行日期。为了给法律的实施留出一定的准备时间,我国多数法律都规定法律公布一段时间后的一个具体日期作为法律的施行日期,《密码法》亦采用这一方式。