

公安机关网络空间安全监督检查办法

（征求意见稿）

第一条 为规范公安机关对网络空间安全的监督检查工作，维护国家安全、社会稳定和公共利益，预防、治理网络违法犯罪，保障公民、法人和其他组织合法权益，根据《中华人民共和国警察法》《中华人民共和国网络安全法》《中华人民共和国数据安全法》《中华人民共和国个人信息保护法》等有关法律、行政法规规定，制定本办法。

第二条 本办法适用于公安机关依法对网络运营者、数据处理者、个人信息处理者等履行法律法规规定的网络安全、信息安全、数据安全义务情况开展的监督检查。

本办法所称网络空间安全，包括网络安全、信息安全、数据安全。

第三条 公安机关开展网络空间安全监督检查，应当遵循依法科学管理、保障和促进发展的方针，严格遵守法定权限和程序，改进执法方式方法，全面落实执法责任。

公安机关应当建立并落实网络空间安全监督检查制度，自觉接受被检查对象和人民群众的监督。

第四条 公安机关可以通过网络信息巡查、信息审核能力测

试、漏洞扫描等不危害网络空间安全的方式，对被检查对象的网络安全、信息安全、数据安全等情况进行线上巡查，以发现风险隐患。对线上巡查发现的风险隐患，应当通过现场检查等方式进行线下核查。

上级公安机关可以组织开展本辖区范围内的线上巡查。开展信息审核能力测试的，应当事先告知被检查对象巡查时间、巡查范围等事项。

设区的市级以上公安机关可以通过漏洞探测、渗透性测试等方式，对本辖区范围内关键信息基础设施以外的网络设施、信息系统进行网络空间安全监督检查，但应当事先告知被检查对象检查时间、检查范围等事项，不得干扰、破坏被检查对象网络设施、信息系统的正常运行。

第五条 开展网络空间安全现场检查，由被检查对象运营机构所在地县级以上公安机关实施。被检查对象为个人的，可以由其经常居住地公安机关实施。

前款所称运营机构所在地是指运营者的主营业地，主营业地不明确的，由共同的上级公安机关指定实施监督检查的公安机关。

上级公安机关应当对下级公安机关开展监督检查的工作情况进行指导和监督。必要时，可以提级或者组织有关公安机关开展监督检查。

第六条 公安机关根据网络空间安全防范需要，可以对下列

对象依法开展监督检查：

（一）提供互联网接入、数据中心、内容分发、域名服务、信息服务等的互联网服务提供者；

（二）公共上网服务提供者；

（三）网络运营者及其建设者、维护者；

（四）关键信息基础设施运营者及其建设者、维护者；

（五）网络产品、服务的提供者；

（六）数据处理者；

（七）个人信息处理者；

（八）其他依法可以监督检查的对象。

对开展前款规定的服务未满一年的，两年内曾发生过网络安全、数据安全事件、违法犯罪案件的，或者因未履行法定网络安全、信息安全、数据安全义务被予以行政处罚的，应当开展重点监督检查。

第七条 公安机关应当对被检查对象履行法定网络安全、信息安全、数据安全义务等情况进行监督检查，重点检查以下内容：

（一）是否依法办理联网单位备案手续，并报送接入单位和用户基本信息及变更情况；

（二）是否依法制定并落实网络安全、信息安全、数据安全管理制度和操作规程；

（三）是否依法记录并留存用户注册信息和上网日志信息；

（四）是否依法履行网络安全等级保护定级备案、等级测评、

建设整改、自查等安全保护义务；

（五）是否依法履行关键信息基础设施安全保护义务；

（六）是否依法采取防范计算机病毒和网络攻击、网络侵入等技术措施；

（七）是否依法针对网络安全漏洞、隐患采取相应的整改措施，消除风险隐患；

（八）是否依法在公共信息服务中对法律、行政法规禁止发布或者传输的信息采取防范措施；

（九）是否依法落实算法安全主体责任，建立健全算法推荐管理制度和技术措施；

（十）是否依法履行数据安全、个人信息保护义务；

（十一）是否依法为公安机关维护国家安全、防范调查恐怖活动、侦查犯罪等提供技术支持和协助。

第八条 在国家重大安全保卫任务期间，对与国家重大安全保卫任务相关的网络运营者、数据处理者、个人信息处理者，公安机关可以重点对下列内容开展专项监督检查：

（一）是否制定重大安全保卫任务所要求的工作方案，明确安全责任分工并确定安全管理人员；

（二）是否组织开展网络安全、信息安全、数据安全风险评估，并采取相应风险管控措施，堵塞安全漏洞隐患；

（三）是否制定网络安全、信息安全、数据安全应急处置预案并开展应急演练，应急处置相关设施是否完备有效；

（四）是否依法采取重大安全保卫任务所需要的其他网络安全、信息安全、数据安全防范措施；

（五）是否依法向公安机关报告网络安全、信息安全、数据安全事件及处置情况。

对防范恐怖袭击的重点目标的安全监督检查，按照前款规定执行。

第九条 公安机关开展网络空间安全监督检查，不得干扰被检查对象的正常运营。

公安机关对网络安全等级保护三级以上的网络运营者、关键信息基础设施运营者，应当每年开展一次现场检查。

必要时，公安机关可以开展专项监督检查。

第十条 公安机关应当会同有关主管部门建立健全网络空间安全监督检查的协作配合机制，加强监督检查的统筹协调、协同配合、信息沟通，合理确定现场检查的频次、范围、方式，视情开展联合监督检查，避免重复检查、交叉检查，最大程度减少被检查对象的负担。

第十一条 公安机关开展网络空间安全现场检查，人民警察不得少于二人，并应当出示人民警察证和县级以上公安机关出具的监督检查通知书。

第十二条 公安机关开展网络空间安全现场检查，可以采取下列措施：

（一）进入营业场所、机房、工作场所；

(二) 问询被检查对象的负责人或者网络安全、信息安全、数据安全管理人员，要求对监督检查事项说明情况；

(三) 查阅、复制与监督检查事项相关的信息；

(四) 查看安全保护技术措施运行情况；

(五) 开展漏洞探测、渗透性测试等技术检测。

第十三条 公安机关开展网络空间安全监督检查，可以委托具有相应技术能力的网络安全服务机构或专门人员提供技术支持，并向上一级公安机关备案。

公安机关应当对参与漏洞探测、渗透性测试的网络安全服务机构及其工作人员开展背景审查，并进行全流程的安全管理。

第十四条 被检查对象应当依照法律、行政法规的规定，对公安机关监督检查给予必要的支持、协助。

第十五条 公安机关开展网络空间安全现场检查，应当制作监督检查记录，并由开展监督检查的人民警察和被检查对象的负责人或者网络安全管理人员签名。被检查对象的负责人或者网络安全管理人员对监督检查记录有异议的，应当允许其作出说明；拒绝签名的，人民警察应当在监督检查记录中注明。

公安机关远程开展漏洞探测、渗透性测试等监督检查，应当制作监督检查记录，并由二名以上开展监督检查的人民警察在监督检查记录上签名。

委托网络安全服务机构、专门人员提供技术支持的，技术支持人员应当一并在监督检查记录上签名。

监督检查过程中形成的文件材料，应当按照规定立卷存档。

第十六条 公安机关在监督检查中发现被检查对象存在网络安全、信息安全、数据安全等风险隐患的，应当督促指导其采取措施消除风险隐患，并在监督检查记录上注明。

被检查对象存在不依法履行网络安全、信息安全、数据安全义务等情况的，公安机关依照《中华人民共和国网络安全法》《中华人民共和国数据安全法》《中华人民共和国个人信息保护法》等法律法规，追究其法律责任。

第十七条 公安机关在监督检查中，发现被检查对象存在网络安全、信息安全、数据安全风险隐患，尚不构成违法犯罪的，可以按照下列程序予以提示或者通告：

（一）由县级以上公安机关向被检查对象发放公安提示函，督促其采取安全防范措施；

（二）由设区的市级以上公安机关向行业主管部门发放公安提示函，督促其加强本行业网络安全、信息安全、数据安全监督管理；

（三）由省级以上公安机关向社会发布不指向具体被检查对象的公安通告，提示网络安全、信息安全、数据安全风险隐患，督促社会公众采取防范措施。

第十八条 公安机关在网络空间安全监督检查中，发现第三级以上网络、关键信息基础设施、重要数据存在重大安全风险隐患的，应当及时通报同级行业主管部门、网信部门。

发现重要行业或者本地区存在严重威胁国家安全、公共安全和
社会公共利益的重大网络安全、信息安全、数据安全风险隐患
的，应当报告同级人民政府和上级公安机关，并按照规定发布公
安提示或者通告。

第十九条 省级以上公安机关在履行网络安全、信息安全监
督管理职责中，发现存在较大安全风险或者发生安全事件的，可
以对该网络运营者的法定代表人或者主要负责人进行约谈。

县级以上公安机关在履行数据安全监督管理职责中，发现数
据处理、个人信息处理活动存在较大安全风险或者发生数据安
全、个人信息安全事件的，可以对有关组织、个人进行约谈。

被约谈对象应当按照法律法规要求采取措施进行整改，消除
网络安全、信息安全、数据安全等风险隐患。

第二十条 公安机关及其工作人员和受委托提供技术支持的
网络安全服务机构及其工作人员，应当保守监督检查中知悉的国
家秘密、工作秘密、商业秘密以及个人信息、隐私，不得泄露、
出售或者非法向他人提供。

在监督检查中获取的信息、资料，只能用于维护网络空间安
全的需要，不得用于其他用途，不得提供给其他组织、个人。监
督检查完毕后，参与监督检查的网络安全服务机构及其工作人员
应当将获取的信息、资料交由公安机关保管，或者按照公安机关
要求进行删除、销毁。

第二十一条 公安机关及其工作人员在网络空间安全监督检

查中玩忽职守、滥用职权、徇私舞弊的，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；构成犯罪的，依法追究刑事责任。

第二十二条 受公安机关委托提供技术支持的网络安全服务机构、专门人员，从事非法侵入被检查对象网络、干扰网络正常功能、窃取网络数据等危害网络空间安全的活动，窃取或者以其他非法方式获取、出售或者向他人提供在工作中获悉的国家秘密、工作秘密、商业秘密、个人信息的，依法予以处罚；构成犯罪的，依法追究刑事责任。

第二十三条 本办法自 2026 年 X 月 X 日起施行，2018 年 9 月 15 日发布的《公安机关互联网安全监督检查规定》（公安部令第 151 号）同时废止。