服务需求

一、项目概述

项目背景：依据中华人民共和国《国家网络安全法》《信息安全等级保护管理办法》及《信息安全技术 网络安全等级保护基本要求》GB/T 22239-2019 等法律法规要求，上海市大数据中心信息化服务第一分中心（简称“一分中心”）为满足其服务范围内各委办局的网络安全等级保护测评需求，计划开展信息系统网络安全等级保护测评工作，通过全面评估信息系统的薄弱环节和潜在安全隐患，确保一分中心所辖信息系统的数据安全、可靠性和稳定性。拟通过公开招标方式，选择优质的服务商提供网络安全等级保护测评服务。

服务期限：自合同签订之日起至 2026 年 12 月 31 日

服务地点：上海市大数据中心信息化服务第一分中心

预算总金额：7,180,612 元

当年度预算金额：7,180,612 元

采购金额（最高限价）：7,180,612 元

组织形式：集中采购

采购方式：公开招标

面向企业类型：面向全部类型

是否接受联合体投标：否

二、服务范围

一分中心按照中心网络安全相关工作要求，以重要信息系统网络安全综合保障为重点，通过开展网络安全等级保护测评服务项目，根据《国家网络安全法》《信息安全等级保护管理办法》等的精神和要求，对测评范围的信息系统进行梳理，按照其定级备案情况，依据GB/T 22239-2019《信息安全技术网络安全等级保护基本要求》安全标准的安全保障要求，明确网络安全工作职责分工，切实推进一分中心2026年度网络安全各项工作有序开展，落实信息系统等级保护测评工作。

一分中心2026年等保测评项目中服务范围需覆盖市大数据中心一分中心运维信息系统，完成招标项目要求的网络安全等级保护测评工作。

2.1 系统重要等级

本项目需按照等保测评要求为以下系统提供网络安全等级保护测评服务，此外，需根据实际需求情况，若年度内有新划转的信息系统，提供数量不少于39个的测评服务。具体以实际服务范围为准:

序号	团队	大系统名称	等保级数
1	发改委（含粮食物资储备局）和统计局团队	上海市发改委门户网站	第三级
2		上海市粮食和物资储备局业务管理平台	第三级
3		上海市粮食和物资储备局智慧决策平台	第三级
4		上海市粮食和物资储备局门户网站	第二级
5		国家级普查、调查数据处理系统	第三级
6	国资委、科委和地方金融监	市地方金融监管局金融服务信息系统	第三级
7		市地方金融监管局监管信息系统	第三级

8	管局团队	科技政务服务系统	第三级
9		科技管理信息系统	第三级
10		上海市科委分布式网上业务服务系统	第三级
11	财政局团队	市财政局基础网络平台	第三级
12		上海市预算管理一体化信息系统	第三级
13		上海市政府采购云平台	第三级
14		上海市财政综合办公系统	第三级
15		非税收入管理系统	第三级
16		上海市财政局门户网站	第三级
17	市场监管局（含药监局）团队	市场监管一网统管大系统	第三级
18		市场监管质量发展与技术基础大系统	第三级
19		市场监管一网通办大系统	第三级
20		市场监管数据慧治大系统	第三级
21		市场监管协同办公大系统	第三级
22		互联网+监管系统	第三级
23		市药品监管局药品监管大系统	第三级
24		市药品监管局协同办公大系统	第三级
25		市药品监管局一网通办大系统	第三级
26		市药品监管局风险管控大系统	第三级
27		市药品监管局公众服务大系统	第三级
28	经信委和商务委团队	市经信委政务办公大系统	第二级
29		上海市经济和信息化委员会门户网站	第三级
30		市商务委行业通管系统	第三级
31		市商务委公共服务系统	第三级
32		市商务委门户网站	第三级
33		市商务委数据中台	第三级
34	审计局和知识产权局团队	上海市知识产权局数字知识产权一体化管理系统	第二级
35		上海市知识产权局网站	第三级
36		上海市知识产权信息工程	第二级
37		审计信息化系统	第三级
38		上海数智审计监督系统	第三级
39		上海市审计局门户网站	第三级

2.2 等保测评服务内容

一分中心 2026 年等保测评项目服务内容包含不少于 39 个应用/信息系统（单个系统可能包含多个域名或者应用模块），按照中心等级保护测评工作相关要求，参照信息系统的用途及功能描述，完成信

息系统网络安全等级测评要求的相关工作，交付相关材料。

应根据各委办团队实际情况，按需提供相关服务。

三、等保测评服务需求

本项目应按《信息安全技术 网络安全等级保护基本要求》GB/T 22239-2019 标准，展开如下服务：

3.1 等级保护咨询服务

1、协助一分中心安全团队针对下属 6 个信息化服务团队的信息系统及相关资产进行梳理，收拢、确认网络安全等级保护备案系统与项目信息系统的对应关系，明确系统备案名称，系统测评对象等信息。

2、根据等级保护测评要求，结合信息系统业务场景，对不少于 39 个信息系统在等保定级测评环节提供咨询服务。包括但不仅限于分中心测评实施方案制定，测评进度跟进、统计、上报，测评全过程沟通协调工作等。

3、按照分中心实际需求提供应急响应相关服务。

3.2 等级保护测评服务

1、完成不少于 39 个信息系统的等级保护测评工作。开展现场测评，协助信息化团队对风险问题进行安全整改，直至被测对象符合中心等保测评分数要求。

2、对测评对象进行初测。对初测信息系统发现的风险问题提供

整改建议，并完成复测，确保信息系统通过等保测评。

3、供应商根据信息系统网络等级保护测评实际情况，按照等保测评实际要求提供相关的服务。

4、等级保护测评服务要求获得相关业务系统的等级保护备案证明和测评报告。

3.3 交付物

按照一分中心 2026 年等级保护测评工作要求，完成不少于 39 个信息系统等级保护测评服务（具体信息系统清单以实际需求为准，由采购方确认），出具符合规范的相关报告。

服务方式：远程与现场相结合的方式。

服务交付物：《等保测评服务总体实施方案》、《等保测评差距分析及整改建议报告》、《等级保护测评报告》、《等保测评服务年度总结报告》。

四、培训服务需求

4.1 培训内容需求

提供不少于一次等级保护测评培训服务，覆盖一分中心及 6 个信息化服务团队等级保护测评相关人员。

依据采购人需求，提供等保基础知识、等保相关政策与法规、等保测评基本要求、等保测评相关标准等专业培训，并制定详细的用户培训方案，包含培训内容、培训方式，培训时间等内容。

4.2 交付物

服务交付物:《等保测评培训服务方案》《等保测评培训课件》。

五、服务质量考核要求

5.1 考核标准

1、 在指定时间内完成信息系统等保差距分析。

2、 在规定的时间内，提交等保测评整改建议报告、完成等保测评报告。

3、 提交的等保测评相关文档完整度和准确性大于95%。

4、 等保测评环节要求的咨询服务响应率=100%,服务响应时间小于5分钟，人员到场时间小于2小时。

5、 在服务期间内,服务清单中信息系统等保测评覆盖率=100%。

5.2 考核方式

1、在履行期限内，服务提供方应当在服务期限过半及服务验收前以书面形式向用户方递交信息系统等保测评服务执行进度汇总报告。

2、服务提供方应当在服务期限结束两个月前以书面形式提交等级保护测评报告等相关材料，用户方在收到服务报告后，在服务期限结束前完成服务质量考核。

3、如果由于服务提供方原因，等级保护测评报告不符合国家相

关标准要求致使未能通过考核，服务提供方应当自收到通知之日起10个工作日内及时整改，直至服务完全符合要求。

5.3 考核结果处置

服务质量的考核结果将作为确认甲方需支付的最终合同总价的依据之一。就甲方需支付的最终合同总价，服务质量考核结果为优秀和良好的按合同金额 100%支付，服务质量考核结果为一般的按合同金额97%为上限支付。

六、验收要求

等级保护测评服务期限结束两个月前，服务提供方应当以书面形式向用户方提交《等级保护测评报告》及相关材料。用户方在收到服务提供方提交的等级保护测评资料（服务周期内的服务过程文档和服务总结报告等）后，在服务期限结束前完成验收。如属于服务提供方原因致使等级保护测评服务未能通过验收的，服务提供方应当在 10个工作日内进行整改，并自行承担等级保护测评相关费用，再次接受用户方的验收，直至符合约定要求。

七、付款方式

本项目采用下列方式付款：

①合同签订生效后且甲方收到乙方开具的等额发票后的 10个工作日内，支付合同总价款的70%；

②本项目通过最终验收且甲方收到约定的项目工作成果、乙方开具的等额发票后的10个工作日内，支付合同总价款的30%。

八、服务组织和人员要求

8.1 服务组织要求

具有类似业绩的优先考虑。

8.2 服务人员要求

本项目需配备等级保护咨询服务及等级保护测评的技术支持人员。选派在项目服务方面富有经验的团队人员负责项目的等保测评服务工作，项目团队应配置对应的人员，团队应至少配备15人，其中，1名项目经理：负责等保测评项目的协调、处置和管理工作；14名安全服务工程师；按照项目实施要求提供相应服务，并至少1人提供5×8小时现场驻守。具体人员要求如下表所示：

角色	主要职责	人数	人员要求	驻场要求
项目经理	负责项目服务工作的协调、处置，团队人员管理。	1	具备硕士及以上学历，5年及以上政务类信息系统等保测评项目管理经验；具备高级职称、信息系统项目管理师证书。	不驻场
安全服务	负责等级保护服务相关工	14人	等保测评工程师团队全	至少1

工程师	作内容的实施。		员具备等保测评师中级及以上证书;3 年以上政务类信息系统等保测评服务项目经验。	人驻场

需根据人员要求，附上述人员毕业证书、职称及职业资格证书及开标前三个月中任意一个月为上述人员依法缴纳社保费的证明。

九、应急服务

1、服务提供方坚持主动预防、迅速高效的原则，紧密结合实际情况， 提供 7*24 小时全天候应急响应服务。

2、中心安全事件应急响应等级分为Ⅳ级、Ⅲ级、Ⅱ级、Ⅰ级，分别对应一般、较大、重大和特别重大安全事件。中心安全事件分级原则详见附件一。

当：

a、发生Ⅰ级（特别重大）故障后 0.5 小时内无法通过电话或远程支持服务排除故障，如采购人要求提供现场支持，服务提供方应 2 小时内到达用户现场；

b、发生Ⅱ级（重大）故障后 0.5 小时内无法通过电话或远程支持服务排除故障，如采购人要求提供现场支持，服务提供方应 3 小时内到达用户现场；

c、发生Ⅲ级（较大）故障后 1 小时内无法通过电话或远程支持服务排除故障，如采购人要求提供现场支持，服务提供方应 3 小时内到达用户现场；

d、发生Ⅳ级（一般）故障后 1 小时内无法通过电话或远程支持服务排除故障，如采购人要求提供现场支持，服务提供方应 4 小时内到达用户现场。

4、如发生故障，服务提供方应严格按照制定的应急预案中故障处理流程实施故障排除操作。

5、当故障排除操作全部完成后，服务提供方应向采购人提交运维故障报告，经采购单位验证通过后签字确认并归档保存，同时组织更新相关文档。

6、如遇有重大事件（包括汛期、节假日、政治军事活动等），服务提供方应科学编制安全保障方案，并根据采购人需要提供现场保障服务。

十、网络和数据安全管理要求

服务提供方在提供等保测评服务过程中应严格按照“同步规划、同步建设、同步使用”原则落实项目安全技术措施，将系统安全运营相关监控措施纳入方案。

若等保测评服务为涉密项目，服务提供方还须参考市保密部门管理要求，严格按照国家《中华人民共和国保守国家秘密法》等相关保密法律法规进行管理，并接受中心保密延伸检查。

1、在提供等保项目服务过程中，服务提供方应在中心限定的办公区域内、访问或使用中心限定的信息资产（包括但不限于场地办公设施、计算机、服务器等），并在规定的安全环境中进行数据处理、

开发测试、运维监控等活动，遵守环境安全监控的要求，在开发测试工作中，不得使用真实生产数据、不得越级操作；

2、提供等保项目服务过程中若涉及开源软件、组件等产品的使用，服务提供方应在使用前向中心提供项目涉及产品的完整清单，并附相应产品的漏洞扫描报告、安全评估报告等证明材料，审核通过后方可使用；

3、服务提供方提供等保项目服务过程中须保障现有系统的网络通畅、系统可用和数据安全。严格落实网络和数据安全防护能力、密码应用、信创应用等运维、运营工作要求，配合开展系统等级保护定级、密码应用安全性评估等工作；

4、服务提供方在提供等保项目服务过程中，被中心或第三方测评机构检测出安全漏洞、等保/密评测评未通过，服务提供方须在规定时限内完成整改并提供复测报告，逾期未整改到位的有权按中心相关管理规定作出处罚；

5、服务提供方须提供自身的网络与数据安全管理制度、保密管理制度，并在中标后提供人员、财务及安全管理情况报告，发生造成中心及项目受影响的变动，应及时向中心报告；

6、服务提供方中标后与中心签订保密协议，同时服务提供方应对项目相关人员开展安全培训，并与该项目人员的签订保密协议，且保证用于项目实施工作的相关终端安装正版杀毒软件及防火墙；

7、提供等保项目服务过程中，服务提供方需要对收集到的所有信息严格管理，严禁在网络上传播、散布和出售，牟取商业利益；服

务提供方人员不得以任何方式泄露、公开或传播项目涉及的内容及成果；不得非法篡改数据、非法入侵中心网络，不得影响数据的完整性及可用性；不得留存任何安全风险隐患；参与项目建设与质保、维修的个人，不得私自拷贝和留存上述信息副本；

8、指定专人负责项目实施过程中的安全工作，接受中心数据安全部门的直接管理和考核，协助开展安全检查等工作；

9、服务提供方若需互联网端功能测试，应经中心批准同意，结束后应及时关闭测试系统，删除测试数据，并将结果及时报备中心；

10、服务提供方通过项目获取到的中心数据禁止超过合同限定范围使用，以及违规转发第三方；

11、服务提供方应按中心规定申请数据服务接口，加强认证和鉴权防护，保护中心敏感数据不被泄露；

12、服务提供方禁止将管理后台、数据库服务端口暴露在互联网；

13、加强对项目人员的安全管理。进入项目前，项目人员应参加安全培训并通过考核，接受背景调查，提供本人无犯罪记录证明，与中心签订保密协议。入场前，项目人员应填写入场申请，按需申请系统账号、云桌面账号和工位。入场后，项目人员应在中心规定的安全环境中进行数据处理、开发测试、运维监控等活动，遵守环境安全监控的要求，禁止共用账号、拍照等。在开发测试工作中，依据要求将生产数据脱敏使用，禁止将生产数据导入个人电脑、将中心代码或敏感数据泄露或公开。禁止个人私自搭服务端和共享网络、终端跨互联网和政务外网。禁止在互联网传输中心敏感文件。非驻场人员，按需

提出入网申请，并安装终端管理工具。禁止将中心数据在个人电脑上留存使用，因需求调研或设计获取数据的，禁止将中心敏感数据外发，或存储在共有云上，数据使用后应进行销毁。

14、服务提供方应制定并持续维护系统相关数据分类分级表，核查相关网络和数据安全防护情况，确保各项措施满足差异化安全防护要求。

15、服务提供方应配合甲方开展网络和数据安全管理制度规范制定、修订工作，并严格执行甲方安全制度要求。

16、服务提供方应在等保项目服务过程中，配合甲方开展供应链核查，根据甲方威胁情报开展供应链风险排查，及时升级、维护风险组件或软件，实时维护软件供应链物料清单及信息化资产底账。

17、服务提供方应落实业务连续性、数据流转等情况的监测工作，定期核查相关日志记录，及时发现异常访问、权限变动及数据流转异常等问题，开展应急处置，采取安全加固措施，确保网络和数据安全。

18、服务提供方应持续优化系统运行环境安全配置和安全管理策略，定期组织系统基线核查、账号及数据访问权限核查等安全自查，及时整改在安全自查、季度检查、众测等安全检查工作中发现的安全漏洞和问题隐患。乙方应配合甲方落实等保、密评、数据安全风险评估等安全测评工作，确保网络和数据安全管理工作符合要求。

19、服务提供方应根据信息系统实际，修订网络和数据安全应急预案，建立应急响应机制，定期开展系统备份和数据备份操作，组织安全事件应急演练和数据备份恢复演练，常态化落实应急响应以及重

大活动时期保障工作，确保系统安全、稳定运行。

20、服务提供方应按照甲方场地及人员管理制度，加强人员管理，并配合甲方落实人员背调、入离场、终端管理、网络限制、数据权限最小化等管控措施。

十一、网络和数据安全处罚措施

如供应商在服务周期内发生网络和数据安全工作违约情况，对中心系统造成网络安全或数据安全影响的，按照引发的安全事件等级和次数，中心将采取以下处罚措施，具体处罚措施由中心安全管理部门确定：

（1）限期整改；

（2）约谈企业负责人；

（3）扣除项目服务费用的 1%-3%；

（4）上报主管部门，必要时终止项目合同并追究相关刑事责任。

供应商应承担服务过程中出现赔偿责任（包括但不限于直接损失、间接损失、律师费、诉讼费/仲裁费、调查费、公证费、保全保险费/担保费）。

实施分包服务的项目，由分包商产生的安全责任问题，供应商应与分包商承担连带责任。

事件类型与等级及与之相应的处罚措施详见附件二。

十二、备份与恢复

1、服务提供方在开展等保测评及相关服务前，需告知用户信息系统可能遇到的数据安全风险，提示用户做好数据备份与恢复工作。

2、服务提供方需配合用户采取应对措施以规避服务过程中可能出现的信息系统数据安全风险。

十三、项目的变更、解除和终止

如果服务提供方丧失履约能力、发生资不抵债或进入破产程序，招标单位可在任何时候以书面形式通知服务提供方终止本项目的执行而不给予服务提供方补偿。该终止本项目将不损害或影响招标单位已经采取或将要采取任何行动或补救措施的权利。

如遇国家、行业管理部门等机构的有关标准和规定调整的，导致本项目内容须做相应调整时，双方应按照公平、合理的原则共同协商修改本项目对应的合同的相关条款。

十四、保密责任

1、中标人因履行本项目而知悉的所有数据、信息和资料（包括但不限于账号信息、图表、文字、计算过程、任何形式的文件、访谈记录、现场实测数据、采购人相关工作程序等）以及因履行本项目而形成的数据、信息和任何形式的工作成果，均是采购人要求保密的信息。未经采购人书面同意，中标人不得对外泄露采购人要求保密的信

息，不得用于其他用途，否则中标人需承担由此引起的法律责任和经济责任，包括但不限于直接损失、间接损失、律师费、诉讼费/仲裁费、调查费、公证费等。

2、中标人应采取必要的有效措施保证其参与本项目的人员（包括中标人聘用的人员、借调的人员、实习的人员）无论是在职或离职后，以及中标人的合作方无论是合作中或合作终止后，都能够履行本项目约定的保密义务。若中标人人员或中标人合作方违反保密规定，中标人应承担连带责任。

3、中标人（含中标人参与本项目的人员以及其合作方）未经采购人书面许可，不得以任何形式自行使用或以任何方式向第三方披露、转让、授权、出售与本项目有关的技术成果、计算机软件、源代码、策划文档、技术诀窍、秘密信息、技术资料和其他文件。

4、以上内容的保密期限自中标人知悉保密信息起始至保密信息被合法公开之日止。

5、中标人对采购人提供的临时使用账号要保密，不得公开，对组件开发的账号密码需进行加密，避免信息安全的泄露。未经采购人的同意不得利用采购人的网络及平台进行短信、彩信、微信、邮件等发送,造成的一切后果由中标人负责。

服务过程中标人如出现失、窃密事情，参照网络和数据安全事件处罚措施同等处置，具体处罚措施由中心保密管理部门确定。

十五、违约责任

1、因服务提供方违反保密义务或知识产权约定的，采购人有权要求服务提供方支付本项目费用总额不超过30%的违约金，违约金不足以弥补采购人损失的，采购人有权要求服务提供方赔偿超过部分。若服务提供方违反保密义务，采购人还有权立即单方解除维护服务合同而不承担任何违约责任。

2、服务提供方有下列情形之一，采购人有权解除维护服务合同：

（1）服务提供方在服务周期内出现重大网络与信息安全事故；

（2）因服务提供方服务质量问题导致采购人无法实现目的；

（3）擅自转让或者分包其应履行的义务的；

（4）违反或者未履行维护服务合同约定的其他相关义务，且在采购人要求的合理时间内未能纠正的。

十六、关于转让和分包的规定

本项目不得转让，不得分包。

附件一：中心网络和数据安全事件分级原则

（一）网络安全事件分级原则

网络安全事件分为有害程序事件、网络攻击事件、设备设施故障、灾害性事件和其他网络安全事件等，网络安全事件分为四级：特别重大网络安全事件、重大网络安全事件、较大网络安全事件、一般网络安全事件。

1、符合下列情形之一的，为特别重大网络安全事件：

（1）中心重要信息系统遭受特别严重的系统损失，造成重要业务大面积、长时间（≥60 分钟）瘫痪，丧失业务处理能力。

（2）网站或系统内容遭到篡改，存在以下恶意信息：内容包含但不限于反对宪法所确定的基本原则的；危害国家安全，泄露国家秘密，颠覆国家政权，破坏国家统一的；损害国家荣誉和利益的；煽动民族仇恨、民族歧视，破坏民族团结的；破坏国家宗教政策，宣扬邪教和封建迷信的；散布谣言，扰乱社会秩序，破坏社会稳定的，含有法律、行政法规禁止的其他内容的。

（3）其他对本市国家安全、社会秩序、经济建设和公众利益构成特别严重威胁、造成特别严重影响的网络安全事件。

2、符合下列情形之一且未达到特别重大网络安全事件的，为重大网络安全事件：

（1）中心重要信息系统遭受严重的系统损失，造成重要业务大面积、较长时间（≥30 分钟）瘫痪，业务处理能力受到极大影响。

（2）网站或系统内容遭到篡改，存在以下恶意信息：散布淫秽、

色情、赌博、暴力、凶杀、恐怖或者教唆犯罪的；侮辱或者诽谤他人，侵害他人合法权益的。

（3）其他对本市国家安全、社会秩序、经济建设和公众利益构成严重威胁、造成严重影响的网络安全事件。

3、符合下列情形之一且未达到重大网络安全事件的，为较大网络安全事件：

（1）中心重要信息系统遭受较大的系统损失，造成重要业务局部、一段时间（≥10 分钟）瘫痪，业务处理能力受到影响。

（2）其他对本市国家安全、社会秩序、经济建设和公众利益构成较严重威胁、造成较严重影响的网络安全事件。

4、除上述情形外，对本市国家安全、社会秩序和公众利益构成一定威胁、造成一定影响的网络安全事件，为一般网络安全事件。

（二）数据安全事件分级原则

数据安全事件分为数据篡改事件、数据破坏事件、数据泄露事件、数据非法获取事件、数据非法利用事件和其他数据安全事件等，数据安全事件分为四级：特别重大数据安全事件、重大数据安全事件、较大数据安全事件、一般数据安全事件。

1、符合下列情形之一的，为特别重大数据安全事件：

（1）国家核心数据、50 条及以上本市重要数据、100 万条以上个人信息遭泄露和非法利用，对国家安全构成威胁，对社会秩序和公共利益构成特别严重威胁和造成特别严重影响。

（2）其他对本市国家安全构成威胁，对社会秩序和公众利益构

成特别严重威胁、造成特别严重影响的数据安全事件。

2、符合下列情形之一且未达到特别重大数据安全事件的，为重大数据安全事件：

（1）本市重要数据、50 及以上条敏感个人信息、5000 及以上条个人信息遭泄露和非法利用，对社会秩序和公共利益构成严重威胁和造成严重影响。

（2）其他对社会秩序和公众利益构成严重威胁和造成严重影响的数据安全事件。

3、符合下列情形之一且未达到重大数据安全事件的，为较大数据安全事件：

（1）敏感个人信息遭泄露和非法利用，对个人合法利益构成严重威胁和照成严重影响。

（2）组织关键性商业秘密遭泄露和非法利用，对组织合法利益构成严重威胁和造成严重影响。

（3）其他对社会秩序和公众利益构成较大威胁和造成较大影响的数据安全事件。

4、符合下列情形之一的，为一般数据安全事件：

（1）个人信息遭泄露和非法利用，对个人合法利益构成威胁和照成影响。

（2）组织关键性商业秘密遭泄露和非法利用，对组织合法利益构成威胁和造成影响。

（3）除上述情形外，其他对社会秩序和公众利益构成威胁和造

成影响的数据安全事件。

附件二：网络和数据安全事件处罚措施

序号	类型	负面行为分级情况	追究措施
1	安全事件	1、发生网络安全事件或数据泄露事件，每发生一起，按不同级别进行追究。	见下
2		（1）发生重大（II级）及以上网络和数据安全事件的;	1、限期整改; 2、约谈企业负责人; 3、扣除项目运维费用的 3%; 4、上报主管部门，必要时终止项目合同并追究相关刑事责任。
3		（2）发生较大网络安全和数据事件（III级）的;	1、限期整改; 2、约谈企业负责人; 3、扣除项目运维费用的 2%
4		（3）发生一般网络和数据安全事件（IV级）的。	1、限期整改; 2、约谈企业负责人; 3、扣除项目运维费用的 1%
5		2、被主管部门通报安全事件，每发生一起，按不同级别进行追究。	见下
6		（1）被中央有关部门通报，并核实的。	1、限期整改; 2、约谈企业负责人; 3、扣除项目运维费用的 3%
7		（2）被本市有关部门通报，并核实的。	1、限期整改; 2、约谈企业负责人; 3、扣除项目运维费用的 2%
8		（3）被中心通报，对业务造成影响。	1、限期整改; 2、约谈企业负责人; 3、一个服务周期内累计发生 3 次及以上的，扣除项目运维费用的 1%
9		（4）被重要用户投诉，影响中心形象、声誉。	1、限期整改; 2、约谈企业负责人; 3、一个服务周期内累计发生 2 次及以上的，扣除项目运维费用的 2%

10		3、在日常安全监控和检查中，发现服务厂商建设、运维的系统被非法登陆、信息泄露或篡改、病毒或黑客攻击等安全事件。	1、限期整改; 2、约谈企业负责人; 3、扣除项目运维费用的 2%
11		4、在上级主管单位对中心进行安全检查中，发现问题的。	1、限期整改; 2、约谈企业负责人; 3、在一次检查中发现 2 个及以上高危问题的，扣除项目运维费用的 2%
12		5、未经批准，擅自在各种媒体发表与中心有关的评论或言论。	1、限期整改; 2、约谈企业负责人; 3、扣除项目运维费用的 2%
13	故障	1、发生 A1、A2 级故障。	1、限期整改; 2、约谈企业负责人; 3、扣除项目运维费用的 3%
14		2、发生 B1、B2 级故障。	1、限期整改; 2、约谈企业负责人; 3、一个服务周期内累计 2 次及以上的，扣除项目运维费用的 2%
15		3、发生 C+级故障。	1、限期整改; 2、约谈企业负责人; 3、一个服务周期内累计 3 次及以上的，扣除项目运维费用的 1%
16	漏洞	1、运维项目，未按要求上报产品漏洞情况，未及时更新版本	1、限期整改; 2、约谈企业负责人; 3、每发现一次未上报或未及时更新且存在漏洞发生安全事件的，按事件等级进行项目金额扣除。
17		2、存在漏洞风险，未按要求及时修复漏洞或采取防护措施	1、限期整改; 2、约谈企业负责人; 3、一个服务周期内累计 3 次及以上的中高危漏洞未按期整改的，扣除项目运维费用的 2%; 4、每发现一次未按时修复且发生安全事件的，按事件等级进行项目金额扣除。