服务需求

一、项目概述

项目背景：近年来，网络和数据安全对国家安全和发展的重要性日益凸显，特别是在当前复杂多变的安全形势下，加强密码安全保障工作已迫在眉睫。本项目依据《中华人民共和国密码法》《商用密码管理条例》《信息安全技术信息系统密码应用基本要求》(GB/T39786-2021）《信息安全技术 信息系统密码应用测评要求》（GB/T 43206-2023）《信息系统密码应用测评过程指南》（GM/T 0116-2021）《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》等测评要求，结合上海市大数据中心（以下简称“中心”）密码应用安全性评估实际工作需求，组织开展信息系统密码应用安全性评估工作，通过商用密码应用安全性评估发现信息系统密码应用存在的安全隐患，全面推进中心密码应用安全整改工作，提升信息系统密码应用安全可靠性，确保中心 2026 年密码应用安全性评估工作有序开展。

服务期限：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

预算总金额：1,353,291 元

当年度预算金额：1,353,291 元

采购金额（最高限价）：1,353,291 元

组织形式：集中采购

采购方式：竞争性磋商

面向企业类型：大中小企业及各类供应商

是否接受联合体响应：否

二、服务范围

本项目的服务范围覆盖中心本部下属 5 个部门：办公室（政策法规部）、信息化服务部、数据安全部、应用开发部（门户网站部）、基础设施部的 11 个信息系统所属信息系统商用密码应用安全性评估工作。

序号	单位名称	系统名称	系统数量
1	办公室（政策法规部）	上海市大数据中心协同办公系统	1
2	信息化服务部	上海市大数据中心信息化服务管理系统	4
		进博会数字赋能服务保障一体化系统	
		上海市政务区块链统一平台	
		上海市大数据中心统一运维中枢平台系统	
3	数据安全部	电子政务云安全监管及运营管理综合系统	1
4	应用开发部（门户网站部）	上海市综合监管运行管理系统	3
		市政府门户网站综合管理系统	
		上海市统一综合执法系统	
5	基础设施部	上海市政务外网运行管理和安全监测支撑系统	2
		上海市电子政务灾难备份中心信息系统	

表 二-1-信息系统服务清单

三、服务需求

按照本项目的评估工作要求，完成服务清单内的信息系统密码应用安全性评估服务，出具符合规范的《密码应用安全性评估报告》，提供密码应用技术支撑并协助本项目涉及的部门开展密码应用安全整改工作，协助本项目设计的部门完成 2026 年度密评备案工作，为本项目涉及的部门提供密码安全相关培训服务。

服务方式：远程与现场相结合的方式。

服务交付物：《商用密码应用安全性评估报告》《商用密码应用安全性评估建议》《密码应用安全性评估服务总体实施方案》《密码应用安全性评估服务项目总结报告》。

四、服务质量考核要求

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。

4.1 考核标准

（1）根据项目要求在项目验收前完成相关商用密码应用安全性评估服务工作。

（2）服务提供方应根据本项目的需求，制定详细商用密码应用安全性评估工作计划和方案。

（3）商用密码应用安全性评估项目服务响应率=100%.

（4）文档完整度和准确率大于 95%。

4.2 服务质量要求

（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密码测评服务工作报告，用户方在收到

服务报告后的10个工作日内，完成服务质量考核。

（2）如果由于服务提供方原因致使密码测评服务未能通过考核，服务提供方应当自收到通知之日起10日内及时整改，并自行承担相关整改费用，直至服务完全符合要求。

4.3 考核方式

（1）项目服务过程中，服务提供方应按照中心密码测评工作要求按期完成密码测评服务，服务提供方无法在规定时间内完成密码测评工作，采购方有权利无条件终止合同。

（2）项目服务过程中，中心发现服务提供方密码测评服务不规范等情况，对服务提供方进行警告，服务提供方需在48小时内排查问题并整改，出具相关整改报告。

五、验收要求

商用密码应用安全性评估工作期限终止时，服务提供方应当以书面形式向用户方提交《商用密码应用安全性评估总结报告》。用户方在收到服务提供方提交的密码应用安全性评估资料（服务周期内的服务过程文档和服务总结报告等）后10个工作日内，对服务提供方的工作进行验收。如属于服务提供方原因致使商用密码应用安全性评估服务未能通过验收的，服务提供方应当在15个工作日内进行整改，并自行承担相关商用密码应用安全性评估相关费用，再次接受用户方

的验收，直至符合约定要求。

六、服务组织和人员要求

密码测评服务团队至少配备 7 名密码测评服务人员，其中项目负责人 1 人，测评人员 5 人，档案管理员 1 人。具体人员如下：具体人员如下：

角色	主要职责	人数	人员要求	驻场要求
项目负责人	负责制定项目计划方案，管控项目实施进度、团队人员日常管理，协调处理项目过程中遇到的各类问题。	1	1. 具有密码学或计算相关专业硕士以上学历； 2. 通过国家密码管理局组织的商用密码应用安全性评估从业人员考核； 3. 具备信息安全方面高级职称； 4. 具备 5 年及以上商用密码应用安全性评估经验；	不驻场
测评人员	负责项目实施过程中技术应用的测评工作。	5	1. 通过国家密码管理局组织的商用密码应用安全性评估从业人员考核；	不驻场

			2. 具备人社部门颁发的密码方面中级工程师及以上职称； 3. 具备 3 年及以上商用密码应用安全性评估及经验。	
档案管理员	负责对项目档案的接收、分类、编目等资料档案管理工作。	1	通过国家密码管理局组织的商用密码应用安全性评估人员测评能力考核	根据实际需求进行驻场或者远程服务

表 六-1 人员要求表

七、服务提供方相关要求

1. 供应商须具备经国家密码管理局认定的商用密码检测机构资质证书（业务范围：商用密码应用安全性评估）。

2. 供应商具有类似项目业绩的优先考虑。

八、密码测评工具和模拟测评环境要求

8.1 测评工具要求

本次项目实施过程中所使用的密评工具需形成完整的工具体系，

涵盖检测、编制、评审全流程，所有工具须具备自主知识产权或计算机软件著作权（需提供相关证明材料）。工具需对系统数据进行全面分析，其分析结果作为评估报告的核心佐证依据，确保评估结论的科学性、准确性和权威性。

密评工具包括但不限于以下几类：

（一）核心检测类工具

1、密码算法验证工具，包括国家商用密码 SM2、SM3、SM4 等算法验证；

2、随机数随机性检测工具，包括随机数随机性测试、随机数随机性检测等；

3、数字证书检测工具，包括数字证书格式合规性验证、数字证书验证等；

4、网络安全协议密码套件检测工具；包括但不限于 SSL 协议分析等。

（二）实施管理工具

5、商用密码应用安全性评估工具，包括项目概述、系统资产、测评对象、现场核查、单元测评、整体测评、风险评估、改进建议、总体评价等报告编制功能以及导出项目实施相关材料等。

（三）报告评审工具

6、密评报告评审工具，包括基于图像识别的证据识别、面向文档数据质量检测等技术实现报告评审以及资源消耗智能监管等功能。

8.2 模拟测评环境要求

服务提供方具有密码测评模拟验证环境的能力及相关设备，包括但不限于以下的密码设备：

1、SSL VPN：具有商用密码产品型号证书或商用密码产品认证证书，用于搭建 SSL VPN 网络，模拟 SSL VPN 通信信道的测评。

2、IPSec VPN：具有商用密码产品型号证书或商用密码产品认证证书，用于搭建 IPSec VPN 网络，模拟 IPSec VPN 通信信道的测评。

3、服务器密码机：具有商用密码产品型号证书或商用密码产品认证证书，用于实现重要数据的加解密和完整性保护，模拟重要数据加解密和完整性保护的测评。

4、签名验签服务器：具有商用密码产品型号证书或商用密码产品认证证书，用于实现身份真实性认证、文件和标记的完整性、通信数据机密性和完整性等密码应用功能保护，模拟身份鉴别、控制信息和安全标记的完整性及重要数据传输和存储机密性和完整性、不可否认性等的测评。

5、时间戳服务器：具有商用密码产品型号证书或商用密码产品认证证书，用于实现重要数据的完整性和不可否认性等密码应用功能

保护，模拟重要数据传输和存储的完整性、不可否认性等的测评。

6、电子签章系统：具有商用密码产品型号证书或商用密码产品认证证书，用于实现数据原发行为的不可否认性和数据接收行为的不可否认性等密码应用功能保护，模拟应用和数据安全的不可否认性等。

九、密码应用安全性评估服务管理要求

9.1 密码应用安全性评估服务原则

本项目商用密码应用安全性测评实施方案设计与具体实施应满足以下原则：

1、客观公正原则：测评实施过程中测评人员应保证在最小主观判断情形下，按照测评双方认可的测评方案，基于明确定义的测评方式和解释，实施测评活动。

2、经济性和可重用性原则：测评工作可重用已有测评结果，包括商用密码应用安全性测评结果。 所有重用结果都应以结果适用于待测评系统为前提，并能够客观反映目前系统的安全状态。

3、可重复性和可再现性原则：依照同样的要求，使用同样的测评方法，不同的测评机构对每个测评实施过程的重复执行应得到同样的结果。可再现性和可重复性的区别在于，前者关注不同测评者测评结果的一致性， 后者则与同一测评者测评结果的一致性有关。

4、结果完善性原则：在正确理解《GB/T 39786-2021 信息安全技术信息系统密码应用基本要求》各个要求项内容的基础之上，检测所产生的结果应客观反映系统的运行状态。测评过程和结果应服从正确的测评方法，确保其满足要求。

9.2 密码应用安全性评估服务过程及内容要求

测评服务过程包括四项基本测评活动：测评准备活动、方案编制活动、现场测评活动、分析与报告编制活动。测评方与被测单位之间的沟通与洽谈应贯穿整个测评过程。

1、测评准备活动

本活动是开展测评工作的前提和基础，主要任务是掌握被测信息系统的详细情况，准备测评工具，为编制商用密码应用安全性评估方案做好准备。

2、方案编制活动

本活动是开展测评工作的关键活动，主要任务是确定与被测信息系统相适应的测评对象、测评指标、测评检查点及测评内容等，形成商用密码应用安全性评估方案，为实施现场测评提供依据。

3、现场测评活动

本活动是开展测评工作的核心活动，主要任务是根据商用密码应用安全性评估方案分步实施所有测评项目，以了解被测信息系统真实

的密码应用现状，获取足够的证据，发现其存在的密码应用安全性问题。

4、分析与报告编制活动

本活动是给出测评工作结果的活动，主要任务是根据 GB/T 39786-2021《信息安全技术 信息系统密码应用基本要求》的有关要求，通过单元测评、整体测评、量化评估和风险分析等方法，找出被测信息系统密码应用的安全保护现状与相应等级的保护要求之间的差距，并分析这些差距可能导致的被测信息系统所面临的风险，从而给出各个测评对象的测评结果和被测信息系统的评估结论，形成商用密码应用安全性评估报告。

十、服务内容

信息系统商用密码应用安全性评估的内容包括但不限于以下内容：

1、安全技术测评：包括物理和环境安全、 网络和通信安全、 设备和计算安全、 应用和数据安全等四个方面的安全测评。

（1）物理和环境安全

测评类别	测评单元
安全技术测评-物理	身份鉴别

和环境安全	电子门禁记录数据完整性
	视频记录数据完整性

表 十-1 物理和环境要求

（2）网络和通信安全

测评类别	测评单元
安全技术测评-网络和通信安全	身份鉴别
	通信数据完整性
	通信过程中重要数据的机密性
	网络边界访问控制信息完整性
	安全接入认证

表 十-2 网络和通信安全要求

（3）设备和计算安全

测评类别	测评单元
安全技术测评-设备和计算安全	身份鉴别
	远程管理通道安全
	系统资源访问控制信息完整性
	重要信息资源安全标记完整性

	日志记录完整性
	重要可执行程序完整性、重要可执行程序来源真实性

表 十-3 设备和计算安全要求

（4）应用和数据安全

测评类别	测评单元
安全技术测评-应用和数据安全	身份鉴别
	访问控制信息完整性
	重要信息资源安全标记完整性
	重要数据存储机密性
	重要数据传输机密性
	重要数据传输完整性
	重要数据存储完整性
	不可否认性

表 十-4 应用和数据安全要求

2、安全管理测评：包括安全管理（分为制度、人员、建设和应急四个子模块）的安全测评。

（1）管理制度

测评类别	测评单元
安全管理测评-管理制度	具备密码应用安全管理制度
	密钥管理规则
	建立操作规程
	定期修订安全管理制度
	明确管理制度发布流程
	制度执行过程记录留存

表 十-5 管理制度

（2）人员管理

测评类别	测评单元
安全管理测评-人员管理度	了解并遵守密码相关法律法规和密码管理制度
	建立密码应用岗位责任制度
	建立上岗人员培训制度
	定期进行安全岗位人员考核
	建立关键岗位人员保密制度和调离制度

表 十-6 人员管理

（3）建设运行

测评类别	测评单元
安全管理测评-建设运行	制定密码应用方案
	制定密钥安全管理策略
	制定实施方案
	投入运行前进行密码应用安全性评估
	定期开展密码应用安全性评估及攻防对抗演习

表 十-7 建设运行

（4）应急处置

测评类别	测评单元
安全管理测评-应急处置	应急策略
	事件处置
	向有关主管部门上报处置情况

表 十-8 应急处置

十一、应急服务

11.1 编制应急预案

为了避免测评工作引入新的安全风险，服务方应紧密结合密码测评实际情况，在正式启动网络安全等级保护测评工作前精心编制应急预案，应在风险揭示、工具验证、连续性考虑和工作纪律等方面进行风险规避。

11.2 应急响应要求

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，精心编制并持续完善应急措施。

2、依据故障时间及故障范围划分故障级别，故障级别分为四级，依次为Ⅰ级（紧急）、Ⅱ级（严重）、Ⅲ级（较大）和Ⅳ级（一般），分别定义如下：

Ⅰ级（紧急）故障为工作时间段（8：30——17：30）内大范围故障；

Ⅱ级（严重）故障为非工作时间段（17：30——次日 8：30）内大范围故障；

Ⅲ级（较大）故障为工作时间段（8：30——17：30）内小范围故障；

Ⅳ级（一般）故障为非工作时间段（17：30——次日 8：30）内

小范围故障；

当：

a、发生Ⅰ级（紧急）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（严重）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。

3、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。

4、当故障排除操作全部完成后，服务提供方应向采购单位提交故障报告，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。

5、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，并根据采购单位需要提供现场保

障服务。

十二、网络和数据安全管理要求

服务提供方在提供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。

若运维项目为涉密项目，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、在提供测评服务过程中，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、提供测评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、服务提供方提供测评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;

4、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，并在成交后提供人员、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;

5、服务提供方成交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;

6、提供测评服务过程中，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;

7、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;

8、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;

9、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;

10、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;

11、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;

12、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。

13、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。

十三、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）。

事件类型与等级及与之相应的处罚措施详见附表。

十四、备份与恢复

1、服务提供方在开展商用密码应用安全性评估及相关服务前，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。

十五、保密责任

1、成交供应商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，成交供应商不得对外泄露采购人要求保密的信息，不得用于其他用途，否则成交供应商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、成交供应商应采取必要的有效措施保证其参与本项目的人员（包括成交供应商聘用的人员、借调的人员、实习的人员）无论是在职或离职后，以及成交供应商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。若成交供应商人员或成交供应商合作方违反保密规定，成交供应商应承担连带责任。

3、成交供应商（含成交供应商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成交供应商知悉保密信息起始至保密信息被合法公开之日止。

5、成交供应商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，造成的一切后果由成交供应商负责。

运维过程成交供应商如出现失、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。

附表一：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。