第四章 技术需求

2022年度国家卫生健康委药具管理中心
系统等级保护测评及网络安全服务项目
技术需求书

一、项目概况

（一）项目背景

为贯彻落实《中华人民共和国网络安全法》《中华人民共和国数据安全法》《中华人民共和国密码法》《关键信息基础设施安全保护条例》《关于印发〈信息安全等级保护管理办法〉的通知》（公通字〔2007〕43号）以及《关于推动信息安全等级保护测评体系建设和开展等级测评工作的通知》（公信安〔2010〕303号）等法律和文件规定，按照《GB/T22239-2019信息安全技术网络安全等级保护基本要求》《GB/T 39786-2021信息安全技术信息系统密码应用基本要求》《GB/T 25000.51-2016 系统与软件工程系统与软件质量要求和评价(SQuaRE) 第51部分就绪可用软件产品(RUSP)的质量要求和测试细则》等有关管理规范和技术标准，对中心的5个业务信息系统分别开展安全等级保护测评工作，其中，包括三个等保三级业务信息系统，两个等保二级业务信息系统。同时对其中1个业务信息系统开展商用密码应用安全性评估，对1个业务信息系统开展源代码审计。对中心机房设备及信息系统开展漏扫工作，并组织开展应急演练及网络安全教育培训工作。

（二）项目目标

通过开展网络安全等级保护测评、商用密码应用安全性评估、源代码审计和应急演练工作，了解和掌握上述信息系统的总体安全状况，发现存在的主要问题和薄弱环节，判断系统面临的安全风险，提出风险管理建议，完善信息系统安全防护体系，全面提升系统的安全防护水平，提高信息系统的安全防御能力，更好地保障信息系统的正常运行，以达到国家信息安全相关政策、文件与标准的要求。

（三）工作原则

方案设计与项目实施应满足以下原则：

1、公平原则：实施方应遵循“面向应用、保证质量、客观公正、诚信守诺”的原则开展网络安全等级保护测评、商用密码应用安全性评估、源代码审计和应急演练工作。

2、标准性原则：实施方应依据相关国家标准、行业标准开展网络安全等级保护测评、商用密码应用安全性评估、源代码审计和应急演练工作。要求所使用的标准和规范如与实施方所执行的标准不一致时，按较高标准执行。

3、优质服务原则：实施方应保证提供符合本评测要求和有关标准的优质服务，并确保评测报告符合项目最终验收的所有要求。

4、保密原则：对网络安全服务过程中接触到的各种信息，不得泄漏给任何单位和个人，未经允许不得利用这些信息从事与服务无关的活动。

二、项目内容

（一）项目范围

1.对中心的3个业务信息系统开展三级等保测评工作;对中心的2个业务信息系统开展二级等保测评工作，其中有4个系统部署在云平台上，1个系统部署在自有机房。

2.对中心的1个业务信息系统开展商用密码应用安全性评估工作。

3.对中心的1个业务信息系统开展源代码审计工作。

4.对中心开展网络安全桌面推演应急演练工作。

5.对中心全员开展网络安全教育培训工作。

6.对中心机房及其业务信息系统按季度定期开展安全漏洞扫描检查工作。

（二）项目依据

本次测评应依据但不限于以下政策和标准：

1、《中华人民共和国网络安全法》

2、《中华人民共和国密码法》

3、《中华人民共和国计算机信息系统安全保护条例》（国务院147号令）

4、《国家信息化领导小组关于加强信息安全保障工作的意见》（中办发〔2003〕27号）

5、《关于信息安全等级保护工作的实施意见》（公通字〔2004〕66号）

6、《信息安全等级保护管理办法》（公通字〔2007〕43号）

7、《关于开展全国重要信息系统安全等级保护定级工作的通知》（公信安〔2007〕861 号）

8、《信息安全等级保护备案实施细则》（公信安[2007]1360 号）

9、《计算机信息系统安全保护等级划分准则》（GB 17859—1999）

10、《信息安全技术网络安全等级保护测评要求》（GB/T 28448—2019）

11、《信息安全技术网络安全等级保护测评过程指南》（GB/T 28449—2018）

12、《信息安全技术网络安全等级保护基本要求》（GB/T 22239-2019）

13、《信息安全技术 信息系统密码应用基本要求》（GB/T 39786-2021）

14、《信息系统密码测评要求》

15、《信息系统密码应用测评过程指南》

16、《政务信息系统密码应用与安全性评估工作指南》

17、《信息系统密码应用高风险判定指引》

18、《系统与软件工程 系统与软件质量要求和评价(SQuaRE) 第 51 部分就绪可用软件产品(RUSP)的质量要求和测试细则》（GB/T 25000.51-2016）

（三）服务内容

1、等级保护差距分析

（1）工作内容：开展差距分析，包括但不限于漏洞扫描检查和人工渗透测试等，针对当前的安全状况与安全等级保护要求之间的差距进行分析，明确当前信息系统与等级保护要求的不符合项及差距，并给出整改建议并配合整改，编写信息系统差距分析报告。

（2）交付成果：《信息系统差距分析报告》。

2、整改技术咨询

（1）工作内容：开展整改技术咨询工作，全程协助采购人进行整改工作，使各系统达到等级保护相应级别的要求，并能通过国家相关主管部门的审核。

（2）交付成果：《信息系统整改建议》。

3、等级保护测评

（1）工作内容：开展网络安全测评工作。在整改工作完成后，乙方负责对项目内系统按照国家信息安全等级保护政策、法规和相关标准等要求进行回归测评，对于测评通过，已经达到等级保护二/三级要求的系统出具符合法律法规要

求的测评报告。

（2）交付成果：出具符合国家要求的《网络安全等级保护测评报告》。

4、商用密码应用安全性评估

（1）工作内容：对有关业务信息系统进行密码应用安全性评估包括但不限于：开展差距分析，进行密码应用安全性评估，出具密评报告，提出整改建议，出具整改报告，根据整改报告，编制详细可实施的整体整改方案等相关内容。

（2）交付成果:《密码应用安全性评估报告》、《应用方案及评估意见》、《整改方案》。

5、源代码审计

（1）工作内容：对有关业务信息系统源代码进行安全审计，包括但不限于：行为问题、路径错误、数据处理、处置错误程序、不充分的封装、安全功能、时间和状态、Web 问题和用户界面错误等类别，通过工具扫描、人工代码审计的方式检查系统源代码中的缺点和错误信息，分析并找到这些问题引发的安全漏洞，并提供整改建议。

（2）系统源代码量小于 50 万行。

（3）交付成果:《源代码安全审计报告》、《整改方案》。

6、应急演练

（1）工作内容：以维护采购人重要信息系统的网络及设备的正常运行为宗旨，中标方根据出现的新的网络攻击手段或其他特殊情况制定详细可操作的网络安全应急演练方案。在采购人审核通过后，协助组织进行 1 次网络安全应急演练。

（2）交付成果:《应急演练方案》、《应急演练总结》

7、网络安全教育培训

（1）服务范围：采购方全员。

（2）工作内容：面向采购方全员开展网络安全意识，网络安全法律法规等安全形势的安全培训，培训课时不少于 2 课时（90 分钟）。

（3）交付成果:《安全培训方案》。

8、漏洞扫描

按照采购方要求，每季度开展一次药具管理中心机房设备及业务信息系统安全漏洞扫描检查，并出具检测报告。

9、售后服务

工作内容：网络安全等级保护测评工作完成后，提供1年质保期，质保期内中标方了解到的系统漏洞或安全风险等安全通告信息及时向采购方告知并协助排查相关风险，给出具体的整改建议指导整改。

（四）地点和时限

实施地点：北京

完成时限： 2022年10月31日前完成系统测评、源代码审计及密码测评工作，中心机房设备及信息系统漏扫工作在合同质保期内完成，具体每个项目完成时间甲乙双方协商确定。

三、服务要求

（一）实施要求

1、**投标人必须具备独立完成本项目的能力**

（1）**★具有网络安全等级测评与检测评估机构服务认证证书。**

（2）**★进入国家密码管理局发布的商用密码应用安全性评估试点机构目录。**

（3）**★具有中国合格评定国家认可委员会CNAS认可证书。**

2、投标人应在项目实施周期内，为本项目成立专门的网络信息安全评测项目组，项目组负责人具备网络安全等级测评师（中/高级）、商用密码应用安全性评估能力考试合格证明，小组成员具备网络安全等级测评师中级或初级资格。投标人应提供人员管理及配备方案，并确保人员的稳定。如更换技术服务人员，须由招标方同意并签字确认。

为保证测评工作进度，要求至少配备项目负责人1人、测评人员5-8人（需提供至少近6个月的社保证明）。人员至少包括等级保护高级测评师2名，等级保护中级评师1名，商用密码应用安全性评估师1名，CISP或CISAW或CISSP证书人员1名，培训讲师1名。

投标人需**书面承诺**项目负责人、高级测评师等关键岗位人员全程参与本项目，未经甲方许可不得擅自更换。

人员要求具体如下：

（1）项目负责人

工作经验：5年以上等级测评工作及项目管理经验，具有至少10个第三级

以上信息系统的等级测评经验。

专业知识和技能：熟悉网络安全等级测评，具有丰富的操作系统安全、网络安全、数据库安全和安全管理知识，具有等级保护测评师证书（高级）。熟悉商用密码应用安全性评估政策和标准要求，熟练掌握密码技术，具有商用密码应用安全性评估人员测评能力考核合格证书。

素质能力：具备项目管理和协调能力，工作认真负责，具有高度的责任心，具备信息系统项目管理师资质（中级及以上）。

（2）测评技术人员（等级保护测评师 2-3 名）

工作经验：3 年以上等级测评工作及项目实施经验。

专业知识和技能：熟悉网络安全等级测评，具有丰富的操作系统安全、网络安全、数据库安全和安全管理知识，具有等级保护测评师证书，除项目负责人外，应至少配备 1 名高级测评师，1-2 名中级测评师。熟悉网络安全等级保护测评政策和标准要求，熟练掌握密码技术，具有相应等级的网络安全等级保护测评师资质。

素质能力：具有中级及以上等级保护测评师资质。

（3）测评技术人员（商用密码应用安全性评估人员测评能力考核合格人员 1-2 名）。

工作经验：1 年以上商用密码应用安全性评估工作及项目实施经验。

专业知识和技能：熟悉商用密码应用安全性评估政策和标准要求，熟悉常见的密码算法、密码协议、密钥管理等知识；熟练掌握密码技术在网络、服务器、终端设备、数据库等整个信息系统架构中的应用。

素质能力：具有商用密码应用安全性评估人员测评能力考核合格证书。

（4）测评技术人员（源代码审计人员，具有 CISP 或 CISAW 或 CISSP 证书 1-2 名）。

工作经验：1 年以上网络安全审计工作经验或 3 个源代码审计项目经验。

专业知识和技能：熟悉源代码审计标准要求，熟悉常见的源代码审计知识；有较丰富的源代码审计经验。

素质能力：具有 CISP 或 CISAW 或 CISSP 证书。

（5）培训讲师 1-2 名。

素质能力：具有丰富网络安全培训和授课经验。

3、中标人能按照项目规定的测评要求及进度安排完成等级保护测评、商用密码应用安全性评估、源代码审计和应急演练工作。

4、中标人在进行测评时不能影响信息系统的正常运行和使用，项目实施应依据最新的等级保护、商用密码应用安全性评估、软件测试相关要求和标准进行。

5、中标人必须按照国家网络安全等级保护和信息系统密码应用基本要求标准开展测评工作，并符合《网络安全等级保护测评机构管理办法》(公信安〔2018〕765 号)、《商用密码应用安全性测评机构管理办法》（试行）对测评机构的要求。

6、中标人应遵守国家相关保密法律法规要求，对本项目涉及到的信息化项目内容、方案、数据严格保密。所有参加该项目的技术人员、管理人员都必须与中标人签订保密责任书。

7、测评工具要求：依据网络安全等级保护和商用密码应用安全性评估相关政策和标准要求，在等级保护测评过程中，应采用人工访谈、工具检测、系统配置核查、文档分析的方式分析被测系统在等级保护方面与标准要求的差距；然而，为确保中标机构开展等级保护测评的质量以及提高自动化程度，在工具检测方面，中标单位必须采用符合国家标准的等级保护工具、密码检测合规工具辅助完成测评工作，利用工具软件，提高测评人员工作效率、测评客观公平、测评结果可管理分析汇总。

8、售后技术服务要求：能够提供 5*8 小时（即 5 个工作日*8 小时工作时间）售后技术及保障服务，必要时 4 小时内应到达现场。

（二）其它要求

1、安全调查和测评的过程中，投标人如需采购人工作人员配合，投标人需要详细描述需要配合的内容。如需要采购人工作人员协助完成各种表单，需要详细描述表单的名称、功能及主要表项等等，并由投标人给出具体示例。采购人有权利拒绝提供任何未事先提出的配合要求，由此产生的损失由投标方负全责。

2、本项目中可能需要的硬件平台(如笔记本电脑、PC、工作站等)均由中标人提供，采购人将按照相关要求对设备进行必要的处理。投标人在服务期间未经采购人许可不得将设备带离采购人指定场所，也不得使用任何未经采购人确认的存储设备对测评数据进行复制。

3、投标人需要给出采购人在进行调查、测评和取证时所需要提供的信息列表。经采购人确认后提供给投标人。采购人有权利拒绝提供任何信息列表以外的采购人资产信息。

4、安全测评应按照分层的原则，包括但不限于以下对象：物理环境、网络结构、网络服务、主机系统、数据库系统、密码设备、密码软件模块、应用系统、安全相关人员、处理流程、安全管理制度、安全策略等。

5、投标人应提供本项目的服务方案，包括技术部分和实施部分。技术部分包括整体流程、技术方法和服务方案设计等，需要对每项技术方法的应用位置进行详细描述，技术方案中应详细描述本次网络安全服务采用的测评方式及标准。

6、实施部分包括人员组织、时间安排、阶段性文档提交、验收标准、质量保证和风险规避措施等，需要明确每项工作的时间安排、操作时间和操作人员。安全调查和测评过程中，如需使用安全工具，请在实施方案中详细描述所使用的安全工具（软硬件型号、功能和性能描述）、使用的方式和时间、对环境和平台的要求等。

7、投标人应详细描述安全调查和测评的组织方式，包括组成的人员及分工、测评的过程组织、实施时间安排、测评方式所遵循的标准等。