附件一、宁夏巨灾防范工程商用密码应用安全性评估服务内容

# 商用密码应用安全性评估服务项目

## 项目概况

### 项目基本情况

密码是保障网络与信息安全的核心技术和基础支撑，是解决网络与信息安全问题最有效、最可靠、最经济的手段。《密码法》的颁布实施，从法律层面为开展商用密码应用提供了根本遵循，《国家政务信息化项目建设管理办法》的颁布实施，进一步促进了商用密码的全面应用。

GB/T 39786-2021《信息安全技术信息系统密码应用基本要求》（以下简称《基本要求》），从物理和环境安全、网络和通信安全、设备和计算安全、应用和数据安全、管理制度、人员管理、建设运行、应急处置等8个层面，对系统按照级别进行商用密码应用性安全评估。同时到国家密码管理局备案，国家密码管理局对备案材料和定级准确性进行审核，审核合格后颁发备案证明。备案单位根据信息系统安全等级，按照国家标准开展安全建设整改，建设安全设施、落实安全措施、落实安全责任、建立和落实安全管理制度；并选择符合国家规定条件的商用密码检测机构开展商用密码应用安全性评估；国家密码管理局定期开展监督、检查。

### 项目目标和范围

本项目的宗旨在于通过对宁夏回族自治区地震局信息系统开展商用密码应用安全性评估（以下简称“密评”）工作，通过密评，明确该系统的安全建设现状，检验系统在密码应用方面是否符合国家相关规范和要求，密码技术、密码产品、密码管理等方面是否符合相关标准，找出存在的安全风险，分析安全建设差距，提出安全整改建议，并以此为基础，进一步制定安全建设整改方案，完善保护措施，使该系统满足我国关于密码应用的具体要求，增加信息系统安全的规范性和有效性，提高本单位的安全意识，增强网络的抗攻击的能力，保证被测系统正常运转。

本次密评的范围包括如下系统：

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **评估内容** | **等保级别** | **备注** |
| 1 | OA（含档案系统） | 二级 |  |
| 2 | 地震灾害防御体系信息系统（宁夏震灾防御基础数据库系统、地市级地震灾害防御数据与业务应用服务终端系统） | 二级（拟定） |  |
| 3 | 地震烈度速报与预警系统 | 三级（拟定） |  |
| 4 | 地震灾害防御体系信息系统（宁夏震灾防御基础数据库系统、地市级地震灾害防御数据与业务应用服务终端系统）密码应用方案 |  |  |
| 5 | 地震烈度速报与预警系统密码应用方案 |  |  |

注：以上系统名称以及等保级别以公安机关出具的《备案证明》为主。如果招标要求有缺失，服务商应无条件帮助甲方完成本次商用密码应用安全性评估项目及管理机构备案，不追加任何费用。

### 项目安排

1.密评机构的项目安排应该按照密码应用安全性评估相关标准进行，项目测评周期为45个工作日。

2.在测评活动开展前,需要对被测信息系统的密码应用方案进行评估.通过评估的密码应用方案可以作为测评实施的依据。

测评过程包括4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。

3.测评准各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,为编制密评方案做好准备。

4.方案编制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 成密评方案,为实施现场测评提供依据。

5.现场测评活动是开展测评工作的核心活动,主要任务是根据密评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。

6.分析与报告编制活动是给出测评工作结果的活动,主 要任务是根据密评方案和GM/T0115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,形成密评报告。

### 密评对象

密评对象涉及信息系统部署相关的机房、网络环境、服务器、数据库、应用系统、密码技术产品和密码服务、密钥管理、密码安全管理制度等方面。

统测评范围及对象包括以下几类：

1．机房的电子门禁系统和视频监控系统。

2．整个系统的网络拓扑结构。

3．需要采用密码技术进行安全防护、承载被测系统主要业务或数据的服务器（包括其操作系统和数据库）。

4．需要采用密码技术进行安全防护的服务器及管理终端。

5．需要采用密码技术进行安全防护的业务应用系统。

6．信息安全和密码主管人员、各方面的负责人员、具体负责密码管理的当事人、业务负责人。

7．涉及到信息系统密码安全的所有管理制度和记录。

### 密评依据

密评单位应依据国家密码应用安全性评估保护相关标准开展工作，依据标准包括但不限于如下国家标准：

1.GB/T 39786-2021《信息安全技术 信息系统密码应用基本要求》

2.《信息系统密码应用测评要求》

3.《信息系统密码应用测评过程指南》

4.《信息系统密码应用高风险判定指引》

5.《商用密码应用安全性评估量化评估规则》

6.其它国家法律、法规要求

## 1.2服务要求

### 1.2.1密评指标

根据被测信息系统密码应用安全要求等级，以GB/T 39786-2021《信息安全技术 信息系统密码应用基本要求》中第三级的安全要求为例说明本次密评工作的基本指标。

|  |  |
| --- | --- |
| **测评单元** | **测评指标数量** |
| 技术要求 | 物理和环境安全 | 身份鉴别、电子门禁记录数据存储完整性、视频监控记录数据存储完整性 | 3 |
| 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的完整性、安全接入认证 | 5 |
| 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 | 6 |
| 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、重要数据传输机密性、重要数据存储机密性、重要数据传输完整性、重要数据存储完整性、不可否认性 | 8 |
| 管理要求 | 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 | 6 |
| 人员管理 | 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 | 5 |
| 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 | 5 |
| 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 | 3 |
| 合计： | 41 |

### 1.2.2密评方法

密评的主要方法有：人员访谈、文档审查、实地查看、配置检查和工具测试，具体如下：

1.人员访谈：即通过与受测单位的相关人员进行交谈和问询，了解受测信息系统技术和管理方面的一些基本信息，并对一些测评内容进行确认。

2.文档审查：即审核受测单位提交的有关信息系统安全的各个方面文档，如：受测系统总体描述文件，受测系统密码总体描述文件，安全管理制度文件，密钥管理制度，各种密码安全规章制度及相关过程管理记录、配置管理文档，受测单位信息化建设与发展状况以及联络方式；密码应用方案及评审意见，安全保护等级定级报告，系统验收报告，安全需求分析报告，安全总体方案，自查或上次评估报告等等。通过对这些文档的审核与分析，确认测评的相关内容是否达到安全保护等级要求。

3.实地查看：即现场查看测评对象所处的环境、外观等情况；

4.配置检查：即查看测评对象的相关配置；

5.工具测试：即根据受测信息系统的实际情况，密评人员使用适合的技术工具对其进行测试。

### 1.2.3密评原则

本次商用密码应用安全性评估应满足以下原则：

1、保密原则：对评估的过程数据和结果数据严格保密，未经授权不得泄露给任何单位和个人，不得利用此数据进行任何侵害招标人的行为，否则招标人有权追究责任。

2、规范性原则：评估工作中的过程和文档，具有很好的规范性，可以便于项目的跟踪和控制。

3、可控性原则：评估服务的进度要跟上进度表的安排，保证招标人对于评估工作的可控性。

4、整体性原则：评估的范围和内容应当整体全面，包括国家商用密码应用安全性评估相关要求涉及的各个层面。

5、最小影响原则：评估工作应尽可能小的影响系统和网络，并在可控范围内；评估工作不能对现有信息系统的正常运行、业务的正常开展产生任何影响，保证现有系统24小时的不间断、稳定、安全运行。

6、非高峰期原则：漏洞扫描及工具测试时间，应尽量安排在夜间或法定节假日期间，制定切实可行的测试实施细则；对意外导致的宕机等，应提供应急保障方案，切实保证关键系统能正常工作。

评估单位应严格按照上述原则和商用密码应用安全性评估相关标准开展项目实施工作。

### 1.2.4密评实施内容

1.信息系统备案

完成商用密码应用安全性评估工作后，将评估结果报国家密码管理部门备案。

2.商用密码应用安全性评估

参照GB/T 39786-2021《信息安全技术 信息系统密码应用基本要求》检查被测系统，从物理和环境安全、网络和通信安全、设备和计算安全、应用和数据安全、管理制度、人员管理、建设运行、应急处置进行差距分析，对系统进行初次安全评估。

通过对系统现状的分析和梳理，发现系统现有安全措施与等级保护基本要求的差距，提出安全整改建议，以指导后续安全整改工作。

（1）物理和环境安全：包括身份鉴别、电子门禁记录数据存储完整性、视频监控记录数据存储完整性等内容。

（2）网络和通信安全：包括身份鉴别、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的完整性 、安全接入认证等内容。

（3）设备和计算安全：包括身份鉴别、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等内容。

（4）应用和数据安全：包括身份鉴别、访问控制信息完整性、重要信息资源安全标记完整性、重要数据传输机密性、重要数据存储机密性、重要数据传输完整性、重要数据存储完整性、不可否认性等内容。

（5）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等内容。

（6）人员管理：涵盖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等内容。

（7）建设运行：涵盖制定密码应用方案、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等内容。

（8）应急处置：涵盖应急策略、事件处置、向有关主管部门上报处置情况等内容。

3.咨询服务

提供信息系统的密码安全咨询和整改建议等技术支持服务，涵盖系统建设、运维、管理、技术等相关安全问题；协助开展单位内部网络与密码安全检查工作。

4.安全意识和技能培训

针对技术人员、管理层提供《密码法》和商用密码应用安全性评估的相关培训工作。

5.应急支撑

服务范围涵盖影响系统运行的软硬件故障、网络攻击等事件应急支撑服务。

### 1.2.5项目成果

本次针对本次商用密码应用安全性评估项目，每个系统出具至少以下成果报告一式四份：

《密码应用安全性评估报告》

《密码应用安全整改建议》