**2023年网络安全总集服务需求**

* 1. **项目概况**

根据相关工作要求，省市场监督管理局非涉密业务系统已迁移整合至福州市长乐区数字福建产业园内的数字福建云计算中心（政务云）。福建省市场监督管理局共有20套业务（含智慧一体化平台）部署在省级电子政务云平台上。

目前，我局采购的2022年度网络安全保障服务即将到期，为确保安全的持续性，我局需向专业的安全服务商采购新一年度网络安全保障服务，确保我局云上应用系统安全。

* 1. **技术和服务要求**

**（下文以“★”标示的内容为不允许负偏离的实质性要求）**

* + 1. **网络安全合规体系建设服务**

**1. 等保定级咨询服务（条款1）**

根据等级保护工作需求，协助省市场监督管理局确定信息系统遭受破坏时的影响范围及影响程度，确定信息系统安全保护等级，撰写信息系统定级报告。

**2. 云等保资产分析服务（条款2）**

根据服务范围的应用组成，指导并配合相关运维、应用开发商整理系统的主机、应用及相关联的资产，编制信息系统资产清单及资产报告。

**3. 安全规划与设计服务（条款3）**

对服务范围内信息系统按照相应等级保护要求进行差距分析，形成差距分析报告，对其中不满足或不完全满足要求部分提出整改措施，形成信息系统等级保护整改设计方案。

**4. 云等保安全整改服务（条款4）**

根据差距分析报告及整改设 计方案对服务范围内信息系统协助运维及开发人员进行整改加固，提交信息系统安全整改加固报告。

**5. 云等保管理制度建设辅导服务（条款5）**

辅助省市场监督管理局编写方针、制度、各类记录表格模板在内的三层结构的安全管理制度，达到等级保护测评要求。

**6. 云等保测评辅助服务（条款6）**

托管云平台的等级保护测评数据采集服务，在服务期内，省市场监督管理局如有申请测评，安全服务商将协助配合测评方完成测评中数据采集等工作，直至备案系统通过等级测评。

**7. 云等保备案咨询服务（条款7）**

协助填写《信息系统安全等级保护备案表》等材料，完成备案工作。

**服务频次：按需**

* + 1. **云上安全保障服务**

为福建省市场监督管理局部署在省级电子政务云平台上的51套业务及服务期内新增部署业务系统提供应用安全保障服务。

1. **安全资产管理（条款8）**

根据信息安全等级保护等有关标准，针对云业务系统进行资产全生命周期管理，包括分类调查、分级管理、资产漏洞评估等，提升云上安全资产的管理能力。

**交付成果：《安全资产报告》**

**服务频次：4次/年**

1. **主机安全服务（条款9）**

（1）主机漏洞扫描服务，对云主机、数据库系统进行漏洞扫描；

（2）主机病毒监测服务，云主机部署防病毒软件防范恶意代码，监测主机病毒感染趋势，及时进行安全加固；

（3）安全配置核查服务，对云主机、中间件、数据库系统进行安全配置核查；

（4）主机入侵检测服务，提供主机版入侵检测，实时监测主机安全状态；

（5）主机系统配置加固服务，根据主机安全检测结果进行安全加固。

**交付成果：云主机安全报告**

**服务频次：4次/年**

1. **应用安全服务（条款10）**

（1）web漏洞扫描服务，使用自动化安全工具检测应用系统漏洞，并进行人工验证，提出指导建议；

（2）应用漏洞风险跟踪服务，针对发现的安全漏洞进行修复状态跟踪，通过在线服务提供实时的修复状态信息推送。

**交付成果：应用漏洞扫描报告**

**服务频次：4次/年**

1. **渗透测试服务（条款11）**

安排安全攻防专家针对应用系统开展渗透测试，通过模拟黑客攻击手段，对信息系统配置管理、会话管理、认证、授权、文件上传下载、信息泄露、应用框架、业务逻辑等方面进行测试，全面检测被测系统安全性。根据渗透测试结果，输出渗透测试报告，协助指导用户修复漏洞，并对修复结果进行复查确认。

**交付成果：渗透测试报告**

**服务频次：2次/年**

1. **主动防御服务（条款12）**

通过部署主动防御系统捕获黑客攻击行为，消耗黑客时间精力，增加黑客攻击成本，同时主动防御系统能够获取机器码、网络ID等攻击者特征，可以对攻击者进行溯源甚至反制，达到震慑攻击者保护信息系统的目的。

**服务频次：按需**

1. **安全大数据分析服务（条款13）**

（1）异常流量分析服务，提供可疑访问、恶意访问、安全试探、异常访问数据分析等安全隐患的预警性分析；

（2）定制化告警服务，可定制化构建异常登录、高危漏洞利用、CC攻击、恶意外联等50多个告警场景；

（3）安全隐患分析服务，通过流量分析，结合业务场景，发现应用系统使用过程中产生的安全威胁隐患，及时发出预警；

（4）安全大数据展示服务，多维度可视化展示信息系统安全状况；

（5）威胁预警通告服务，提供实时安全漏洞通知、定期安全通告汇总和安全知识库更新等。

**交付成果：大数据安全分析报告**

**服务频次：4次/年**

1. **网页防篡改服务（条款14）**

针对我局部署在云上的网站（1个节点）页面提供静态网页防护、动态脚本防护等能力，保证原有网页内容不被非法更改。

**交付成果：无**

**服务频次：日常**

1. **安全管理中心（条款15）**

提供安全可视化展示服务能力，展示内容包括安全资产信息、网络攻击态势、主机入侵态势、安全健康度及安全漏洞影响度等。

**交付成果：SaaS化安全态势展示**

**服务频次：日常**

1. **应急保障服务（条款16）**

应急响应处置服务，发生突发事件时，启动紧急事件响应，提供技术支持，以最快速度恢复系统，并提供事后分析，找出网络或系统的安全漏洞。

**交付成果：应急处置报告**

**服务频次：按需**

1. **应急演练指导服务（条款17）**

负责协助省市场监督管理局做好直属单位的年度网络安全应急演练的考核工作，主要针对相关参演单位在事前演练计划的制定、事中演练的开展规范、事后的演练成效等方面进行评判和指导。增强参演人员安全意识，促进人员明确应急职责、熟悉应急流程和应急操作。

**服务频次：1次/年**

1. **安全重保服务（条款18）**

（1）重保时期远程安全保障服务，重保时期，对信息系统启用网站7\*24小时安全监测，并进行远程风险评估；

（2）重保时期现场安全保障服务，重保时期，现场指导对现有安全措施进行有效性检查，根据风险评估结果提供安全整改加固建议，指导值班人员对重点网站主页、安全设备日志进行密切监控，对异常安全告警及时预警处置。

**交付成果：重保时期安全保障报告**

**服务频次：按需**

1. **安全检查专题服务（条款19）**

（1）安全检查协助，协助应对上级监管部门安全检查；

（2）管理制度辅助建设，上级监管部门安全检查期间，协助制定信息安全管理制度。

**服务频次：按需**

1. **安全培训服务（条款20）**

（1）安全意识培训服务，提供安全标准、政策法规解读、信息安全意识、信息安全发展方向、周期性安全服务报告解读等现场培训服务；

（2）安全技术培训服务，提供网站安全防护技术、等保安全建设、网络安全技术攻防、上线测试等现场培训服务。

**交付成果：安全培训PPT**

**服务频次：1次/年**

* + 1. **数据端安全保障服务**

为福建省市场监督管理局部署在省 级电子政务云平台上的数据库数据提供数据库数据安全监管服务，每月提供1份《数据库数据安全监管报告》，包括涵盖**数据资产状态安全监控、数据资产发现与管理、数据业务资产梳理维护和数据资产挖掘及数据资产建模分析等内容。**每年提供1个子系统《数据分类分级规范报告》1份、1个子系统《数据分类分级报告》1份。

1. **数据资产状态安全监控服务（条款21）**

（1）资产态势服务，提供数据资产周期性态势展示。

（2）资产风险分析服务，提供统计并且分析管理范围内业务系统的风险资产信息。

（3）报告分析服务，对数据资产的状态、风险提供分析。

（4）业务系统底账报告人工服务，通过人工整理提供业务系统资产底账报告。

**交付成果**：**每月提供数据库数据安全监管报告（数据资产状态安全监控部分）**

**服务频次：日常**

1. **数据资产发现与管理服务（条款22）**

（1）数据库资产管理服务，对业务系统提供数据库资产发现管理能力。

（2）应用资产管理服务，对业务系统提供应用资产发现管理能力。

（3）网络资产管理服务，对业务系统提供网络资产资产发现管理能力。

（4）终端资产管理服务，对业务系统提供终端资产发现管理能力。

（5）账户资产管理服务，对业务系统提供账户资产发现管理能力。

（6）数据资产发现管理人工服务，为省市场监督管理局的业务资产发现提供人工导入、管理、维护、培训等服务。

**交付成果：每月提供数据库数据安全监管报告（**数据资产发现与管理**部分）12次/年**

**服务频次：日常**

1. **数据业务资产梳理维护服务（条款23）**

（1）资产标识服务，为发现的应用、数据和终端资产提供多标签标识服务。

（2）资产分级服务，根据等保规范对资产进行分类分级。

（3）资产定责服务，按照行政管理部门要求对资产进行分类。

（4）敏感资产管理服务，提供根据行业类型定义敏感资产管理。

（5）业务资产梳理管理人工服务，为省市场监督管理局的业务资产梳理提供人工导入、管理、维护、培训等服务。

**交付成果**：**每月提供数据库数据安全监管报告（数据业务资产梳理维护部分）12次/年**

**服务频次：日常**

1. **数据资产挖掘及数据资产建模分析服务（条款24）**

（1）数据资源管理服务，对采集和主动扫描的资产相关数据提供数据资源管理。

（2）资产发现模型服务，主动扫描、流量分析技术和人工补登的方式进行资产发现。

（3）资产标签管理服务，提供数据资产关联关系标识，实现隐私数据发现。

（4）资产扫描探测服务，发现流量中相应的资产数据、资产访问数据等。

**交付成果：每月提供数据库数据安全监管报告（数据资产挖掘及数据资产建模分析部分）**

**服务频次：日常**

1. **数据日志采集服务（条款25）**

（1）日志数据采集和接收服务，对数据日志进行采集和接收。

（2）日志自动分类服务，对数据日志进行自动分类。

（3）日志清洗服务，对采集的日志数据进行精清洗等操作。

（4）高性能数据加载服务，提供日志数据分布式分发加载服务。

（5）大数据存储管理服务，提供大数据采集入库、数据归集分块存储及数据服务的维护管理。

**交付成果：无**

**服务频次：日常**

1. **数据分类分级服务（试点）（条款26）**

根据目前市场监管数据分类分级管理规则（试行）文件的要求。

（1）数据分类服务，对照总局有关要求，结合省局应用系统开发与数据中心建设进度，开展数据资产分类打标工作，并制定对应的数据分类规范。

（2）数据分级服务，对照总局有关要求，结合省局应用系统开发与数据中心建设进度，开展数据资产分级打标工作，并制定对应的数据分级规范。

**交付成果：子系统《数据分类分级规范》1份、子系统《数据分类分级报告》1份。**

**服务频次：1次/年**

* + 1. **互联网安全防护服务**

1. **互联网网站安全监控服务（条款27）**

（1）提供网站可用性监控服务，对服务范围内的相关网站稳 定性和可用性实时监控分析；

（2）提供网站端口暴露监测服务，服务具有多探测指标、主动探测技术、安全态势分析等功能；

（3）提供域名劫持监控服务，对网站和信息系统首页进行域名劫持探测；

（4）提供网页挂马监控服务，对网站和信息系统挂马分析、预警；

（5）提供网站暗链监控服务，对网站和信息系统页面进行暗链分析、预警；

（6）提供敏感内容监控服务，对关键网页的敏感内容进行监控，识别网站存在政治、低俗等敏感内容情况，并进行邮件或短信预警；

（7）提供实时告警和监控报告服务，推送安全告警信息，并提供网站监控测试报告。

**交付成果：互联网网站安全监控报告**

**服务频次：12次/年**

1. **互联网网站安全漏洞扫描服务（条款28）**

（1）定期提供互联网网站安全漏洞扫描服务；

（2）定期提供互联网网站安全漏洞验证服务；

（3）定期提供互联网网站安全漏洞跟踪服务。

**交付成果：互联网网站安全漏洞扫描报告**

**服务频次：12次/年**

* + 1. **网络防爬虫服务**

**服务范围（条款29）**

（1）涵盖以下2大系统、16个子应用模块,及其拓展、衍生、迭代系统：

|  |  |  |
| --- | --- | --- |
| **系统序号** | **系统名称** | **子应用模块名称** |
| 1 | 国家企业信用信息公示系统（福建） | 企业信息填报 |
| 企业享受扶持信息公示系统 |
| 小微企业库 |
| 福建省工商系统市场主体信用信息公示平台 |
| 2 | 网上工商系统 | 电子营业执照系统 |
| 名 称登记系统 |
| 内资企业登记系统 |
| 外资企业登记系统 |
| 港澳居民个体工商户登记系统 |
| 平潭商事主体名 称自主申报系统 |
| 合同业务申请系统 |
| 流通领域商品质量抽查检验系统 |
| 网络市场监管系统 |
| 经营 范围查询系统 |
| 网上工商应用平台 |
| 企业注销网上服务专区 |

1. 省市场监督管理局后续上线的智慧一体化平台。

**交付成果：防爬虫防护报告**

**服务频次：**4次/年****

* + 1. **华林路办公区安全防护服务**

1. 服务内容：提供省市场监督管理局华林路办公区的上网行为管理、多网隔离、安全防护等服务，并提供相应的日常运维服务。要求本项目服务商免费提供相关设备部署于服务现场。**（条款30）**

2. 服务设备功能及性能要求：**（条款31）**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **序号** | **设备类型** | **设备名 称** | **参数要求** | **数量** |
|
| 1 | 网络行为管理 | 上网行为管理 | (1)性能参数： 1U标准机架，硬盘容量≥1T SATA，单电源，接口≥6千兆电口+2万兆光口SFP+。性能参数≥网络层吞吐量（大包）≥10Gb，应用层吞吐量≥1.5Gb，带宽性能≥1Gb，支持用户数≥3000，包转发率≥132Kpps，每秒新建连接数≥5000，最大并发连接数≥250000。  (2)功能描述：具有用户认证与管理、应用控制、流量管控、行为审计等功能，满足1000个用户终端上网的要求。 | 1 |
| 2 | 网络隔离 | 多网隔离 | (1)性能参数：1U标准机架，网络层吞吐量（大包）≥5.8Gb，应用层吞吐量≥850Mb，带宽性能≥500Mb，IPSEC VPN加密性能（最高性能）≥120Mb，支持用户数≥1500，包转发率≥90Kpps，每秒新建连接数≥3000，最大并发连接数≥150000。  (2)功能描述：与多网隔离认证设备进行安全联动，支持针对不同网络进行不同策略管控，同步多网隔离认证管控设备的用户信息后，针对不同用户组进行策略管控；支持网络增加时多套网络的快速切换，如再增加一套网络，只需针对多网隔离设备进行策略调整即可实现多网切换。 | 1 |
| 3 | 安全防护 | 防火墙 | （1）性能参数：1U标准机架式设备，4个千兆Combo接口（光电复用），千兆电接口≥10个，硬盘≥500G，单电源； 网络吞吐量≥5Gbps， 应用性能≥1.5Gbps， 防护全开性能≥300Mbps， 最大并发连接数≥200万；  （2）功能描述：  ① 支持应用控制策略失效策略检查功能，检测策略可能失效的情况，如规则内容存在冲突、规则生效时间过期、规则超长时间未有匹配等情况；支持应用控制策略模拟匹配功能，支持输入源目的IP、端口，给出最可能的匹配结果，方便排查故障及设备部署前的调试，支持模拟匹配访问时间自定义； ② 支持基于应用类型，网站类型，文件类型进行流量控制，支持基于IP段、时间、国家/地区、认证用户、子接口和VLAN进行流量控制，包含1年防病毒库、IPS攻击特征库、应用特征库+URL特征授权，1年原厂软硬件维保。 | 1 |

**交付成果：提供上表所列设备部署在业主现场照片，并每季度提供1份巡检报告。**

**服务频次：日常**

* + 1. **五四路办公区安全防护服务**

1. 服务内容：提供省市场监督管理局的五四路办公区提供防火墙和交换机等相应设备的服务，并提供相应的日常运维服务。要求本项目服务商免费提供相关设备部署于服务现场。**（条款32）**

2. 服务设备功能及性能要求：**（条款33）**

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **名称** | **说明** | **数量** |
|
| **一、互联网区** | | | |
| 1 | 防火墙1 | （1）性能参数：1U标准机架，千兆电接口≥12个，千兆光接口≥12个，硬盘≥500G，冗余电源；网络吞吐量≥10Gbps，应用性能≥3Gbps，防护全开性能≥400Mbps，最大并发连接数≥200万。  （2）功能描述：  ① 支持应用控制策略失效策略检查功能，检测策略可能失效的情况，如规则内容存在冲突、规则生效时间过期、规则超长时间未有匹配等情况；支持应用控制策略模拟匹配功能，支持输入源目的IP、端口，给出最可能的匹配结果，方便排查故障及设备部署前的调试，支持模拟匹配访问时间自定义； ② 支持基于应用类型，网站类型，文件类型进行流量控制，支持基于IP段、时间、国家/地区、认证用户、子接口和VLAN进行流量控制，包含1年防病毒库、IPS攻击特征库、应用特征库+URL特征授权，1年原厂软硬件维保。 | 1 |
| 2 | 防火墙2 | （1）性能参数：≥1U标准机架，千兆Combo接口（光电复用）≥4个，千兆电接口≥10个，500G硬盘≥500G，冗余电源，网络吞吐量≥5Gbps，应用性能≥1.5Gbps，防护全开性能≥300Mbps，最大并发连接数≥200万。支持IPSECvpn、SSL VPN、L2TP等各种主流VPN功能。  （2）功能描述：  ① 支持应用控制策略失效策略检查功能，检测策略可能失效的情况，如规则内容存在冲突、规则生效时间过期、规则超长时间未有匹配等情况；支持应用控制策略模拟匹配功能，支持输入源目的IP、端口，给出最可能的匹配结果，方便排查故障及设备部署前的调试，支持模拟匹配访问时间自定义；  ② 支持基于应用类型，网站类型，文件类型进行流量控制，支持基于IP段、时间、国家/地区、认证用户、子接口和VLAN进行流量控制，包含1年防病毒库、IPS攻击特征库、应用特征库+URL特征授权，1年原厂软硬件维保。 | 1 |
| **二、政务信息网** | | | |
| 3 | 防火墙 | （1）性能参数：1U标准机架，千兆电接口≥12个，千兆光接口≥12个，硬盘≥500G，冗余电源；网络吞吐量≥10Gbps，应用性能≥3Gbps，防护全开性能≥400Mbps，最大并发连接数≥200万。  （2）功能描述：  ① 支持应用控制策略失效策略检查功能，检测策略可能失效的情况，如规则内容存在冲突、规则生效时间过期、规则超长时间未有匹配等情况；支持应用控制策略模拟匹配功能，支持输入源目的IP、端口，给出最可能的匹配结果，方便排查故障及设备部署前的调试，支持模拟匹配访问时间自定义； ② 支持基于应用类型，网站类型，文件类型进行流量控制，支持基于IP段、时间、国家/地区、认证用户、子接口和VLAN进行流量控制，包含1年防病毒库、IPS攻击特征库、应用特征库+URL特征授权，1年原厂软硬件维保 | 1 |
| 4 | 接入交换机 | （1）端口配置： 10/100/1000Base-T自适应以太网端口≥24个，100/1000 Base-X SFP光口≥4个； （2）功能要求：支持基于端口的VLAN。 | 1 |
| **三、政务外网公用区** | | | |
| 5 | 防火墙 | （1）性能参数：1U标准机架，千兆Combo接口（光电复用）≥4个，千兆电接口≥10个，500G硬盘≥500G，单电源，网络吞吐量≥5Gbps，应用性能≥1.5Gbps，防护全开性能≥300Mbps，最大并发连接数≥200万。  （2）功能描述：  ① 支持应用控制策略失效策略检查功能，检测策略可能失效的情况，如规则内容存在冲突、规则生效时间过期、规则超长时间未有匹配等情况；支持应用控制策略模拟匹配功能，支持输入源目的IP、端口，给出最可能的匹配结果，方便排查故障及设备部署前的调试，支持模拟匹配访问时间自定义； ② 支持基于应用类型，网站类型，文件类型进行流量控制，支持基于IP段、时间、国家/地区、认证用户、子接口和VLAN进行流量控制，包含1年防病毒库、IPS攻击特征库、应用特征库+URL特征授权，1年原厂软硬件维保。 | 1 |

**交付成果：提供上表所列设备部署在业主现场照片，并每季度提供1份巡检报告。**

**服务频次：日常**

* + 1. **长乐机房局域网安全防护服务**

1. 服务内容：为省市场监督管理局的长乐机房省局至国家总局线路提供防火墙的服务，并提供相应的日常运维服务。要求本项目服务商免费提供相关设备部署于服务现场。**（条款34）**

2. 服务设备功能及性能要求：**（条款35）**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **序号** | **设备类型** | **设备名 称** | **参数要求** | **数量** |
| 1 | 安全防护 | 防火墙 | （1）性能参数：1U标准机架，千兆Combo接口（光电复用）≥4个，千兆电接口≥10个，500G硬盘≥500G，单电源，网络吞吐量≥5Gbps，应用性能≥1.5Gbps，防护全开性能≥300Mbps，最大并发连接数≥200万。  （2）功能描述  ① 支持应用控制策略失效策略检查功能，检测策略可能失效的情况，如规则内容存在冲突、规则生效时间过期、规则超长时间未有匹配等情况；支持应用控制策略模拟匹配功能，支持输入源目的IP、端口，给出最可能的匹配结果，方便排查故障及设备部署前的调试，支持模拟匹配访问时间自定义； ② 支持基于应用类型，网站类型，文件类型进行流量控制，支持基于IP段、时间、国家/地区、认证用户、子接口和VLAN进行流量控制，包含1年防病毒库、IPS攻击特征库、应用特征库+URL特征授权，1年原厂软硬件维保。 | 1 |

**交付成果：提供上表所列设备部署在业主现场照片，并每季度提供1份巡检报告。**

**服务频次：日常**

* + 1. **终端安全防护服务**

1. 提供550个终端授权；**（条款36）**

2. 服务功能要求：一体化集中安全管理平台；终端病毒与恶意代码防范；XP系统安全加固；全网终端漏洞统一管理；终端安全管理措施；软硬件资产登记管理。

* 1. **服务交付要求**
     1. **服务交付地点**

云上安全保障服务交付地点：福建省福州市长乐区文武砂镇数字福建产业园东湖一路1号数字福建云计算中心（政务云）机房。

华林路办公区安全防护服务交付地点：福州市鼓楼区华林路147号。

五四路办公区安全防护服务交付地点：福州市鼓楼区五四路358号。

* + 1. **现场驻点要求**

为确保市场监督管理局业务系统安全保障到位、安全事件应急处置高效，要求本项目服务商承诺提供技相应技术服务人员驻点福建省福州市长乐区文武砂镇数字福建产业园东湖一路1号数字福建云计算中心（政务云）机房现场并提供现场安全保障服务。

* + 1. **服务响应时效要求**

数字福建云计算中心：采用现场与远程相结合的方式提供7x24小时事件响应和处置服务，随时进行故障响应与技术支撑。

市场监督管理局办公区：包含华林路办公区和五四路办公区，提供7x24小时事件远程响应和处置服务，若需要本项目服务商提供现场支持的，本项目服务商应在1个小时内提供相关事件的解决方案、3个小时内到达业主指定现场并提供本项目范围内的相关服务。