广东省环境监测中心网络信息安全咨询服务采购项目需求公告

一、采购项目名称：广东省环境监测中心网络信息安全咨询服务采购项目

二、采购品目名称：见附件

三、公告地址：广东省生态环境厅公众网（http://gdee.gd.gov.cn/）

四、供应商资格：

（1）具有独立承担民事责任能力的在中华人民共和国境内注册的法人或其它组织或自然人；

（2）符合《中华人民共和国政府采购法》第二十二条及《中华人民共和国政府采购法实施条例》第十七条的规定：

1)法人或者其他组织的营业执照等证明文件，自然人的身份证明；

2)财务状况报告，依法缴纳税收和社会保障资金的相关材料；

3)具备履行合同所必需的设备和专业技术能力的证明材料；

4)参加政府采购活动前3年内在经营活动中没有重大违法记录的书面声明；

5)具备法律、行政法规规定的其他条件的证明材料。

五、报名应提交的资料

- 1)营业执照等副本复印件和组织机构代码证复印件和税务登记证电子扫描件（或三证合一执照）（原件核查）；

- 2)具备履行项目所必需的设备和专业技术能力的证明材料电子扫描件（原件核查）；
- 3)参加政府采购活动前 3 年内在经营活动中没有重大违法记录的书面声明电子扫描件（原件核查）；

六、符合资格的供应商应当在**2019 年 10 月 23 日至 2019 年 10 月 27 日**期间以电子邮件方式向采购联系人提交报名资料。经过供应商资格预审后，通过预审的供应商提供相应纸质版资料一式四份，本单位将进行评审，选出最符合条件的供应商。

采购单位：广东省环境监测中心

地址：广东省广州市海珠区新港东路磨碟沙大街 28 号

联系人：林先生；联系电话：28368598

邮箱：linzhiling@gdepb.gov.cn

投诉电话：28368508

附件：广东省环境监测中心网络信息安全咨询服务采购项目需求

发布人：广东省环境监测中心

环境统计与信息科

发布时间：2019 年 10 月 23 日

附件：广东省环境监测中心网络信息安全咨询服务采购项目需求

一、项目概况

项目名称：广东省环境监测中心网络信息安全咨询服务采购项目

二、项目背景

为提升中心网络信息安全，及时识别处置系统隐患，委托专业服务机构承担网络信息安全咨询服务工作。

三、采购需求

项目服务周期为：自合同签订起为期 1 年。

服务内容如下：

序号	相关内容		维护要求	服务周期
1	信息系统等级保护服务		配合测评机构对中心网络部署的业务系统进行定级备案和差距测评，根据差距测评报告编制这些系统的安全整改方案，并配合安全整改机构进行安全整改和测评。	按需，共一年
2	安全风险评估服务	系统扫描服务	定期对中心所有系统安全扫描检查，提供扫描评估报告和修复建议(在服务期内提供正版化扫描授权)。 服务方式：现场服务 服务成果要求包含但不限于以下文档： 《中心安全扫描报告》	每月一次
		本地系统检查	定期对操作系统、应用系统进行安全配置、漏洞木马等安全检测,提供整改方案。	每季度一次
		网络设备检测	定期检查网络设备安全配置、漏洞等安全检测，提供整改方案。	每季度一次
3	安全加固		根据每季度的系统安全评估结果，对存在安全威胁的服务器进行安全加固，包括系统漏洞、配置、木马等威胁加固。	每半年一次
4	信息安全专项渗透测试		利用各种主流攻击技术对客户授权指定的应用系统和网络设备做模拟攻击测试 服务方式：现场服务 服务成果要求包含但不限于以下文档： 《渗透测试报告》	每季度一次

序号	相关内容	维护要求	服务周期
5	信息安全应急响应	为重大安全事件提供应急响应服务。提供全年7*24 小时全天候、2 小时到达现场，对安全事件进行应急处置，判断事件级别，中止事件漫延、保护系统和数据安全、分析追踪事件原因并提交事件报告。 按服务成果要求包含但不限于以下文档： 《中心网络信息安全事件应急响应报告》	按需，不限次数
6	安全咨询	在服务期内全年提供信息安全咨询服务，服务内容包含： （1） 根据用户信息化业务发展趋势，协助制定阶段性的安全工作计划； （2） 根据用户网络现状，协助制定年度的网络安全建设计划； （3） 对用户新入网系统架构及网络规划给出合理、具体的规划： （4） 对用户新入网系统选用的网络产品、安全产品给出建议； （5） 对用户新入网系统采用的系统架构给出安全方面的规划方案（包括内部网络）； （6） 配合用户完成系统内部及与之相连的系统结构图和组网图。 （7） 根据上述内容，出具相关报告。	每半年一次
7	安全演练与培训	服务期内提供 2 次网络安全培训，包括安全漏洞发现及修补、病毒发现及防御、安全攻击发现与防御基础、安全相关技术的基础知识。协助信息部门完成网络安全应急演练。 服务成果要求包含但不限于以下文档： 《中心网络信息安全培训 PPT》	每半年一次

四、安全服务管理要求

本次网络信息安全服务项目涉广东省环境监测中心以下基础信息系统设施：信息系统服务器主机、网络安全设备、信息系统软件平台、重要应用信息系统。

在服务过程中发现应用漏洞、主机漏洞、网络安全策略等安全问题后，由安全服务商提供安全整改方案，由业主方组织相关第三方进行修复，修复完成后安全服务商需及时回归评估修复情况。

定期上门服务：每月需安排安全工程师上门日常巡检两次；服务内容包括但不限于设备性能、安全策略设置核查；日志存储分析；安全事件检查等内容。

服务考核：

（1）被信息安全主管部门通报，安全服务商也未在通报之前发现通报问题并告知业主方的，1 次扣 2 分；

（2）单位信息系统出现安全故障，未能及时协助处理的，1 次扣 2 分；

（3）未按要求进行安全通告与咨询服务的，1 次扣 1 分；

考核得分在 95 分或以上时，视为合格，低于 95 分时视为不合格。

惩罚的计算方法如下：考核得分低于 95 分时，每差 1 分扣除合同总额的 1%，惩罚金总额不超过合同总金额的 25%。

五、安全服务工具要求

1、服务过程中所需要的服务工具由投标人自行负责，并保证其所使用的服务相关工具不会产生因第三方提出侵犯其专利权或其它知识产权而引起的法律和经济纠纷，采购人不另行支付任何费用。

2、服务工具应采用成熟、业界著名的商业化的漏洞扫描工具进行安全检查，保证对目标系统无大的影响以及扫描结果的准确性和可信度。投标方必须保证所使用的所有工具和软件不具有所有权和知识产权纠纷，并保证工具和软件可用性和可靠性。由此产生的一切责任由投标方负完全责任。

3、安全服务工具在检查过程中起到良好的辅助作用，检查时使用的工具的配置不得低于投标时所列工具。

漏洞扫描工具要求

设备支持根据网络协议进行通信的客户端和服务端；中间人控制器，对客户端和服务端之间的通信进行监控，并捕获和修改通信数据以对客户端或服务端进

行漏洞挖掘；(提供国家权威部门关于该技术的证明材料，并提供相应材料的网站链接和截图，上述资料需加盖设备生产商公章)

资产发现扫描功能支持配置 IP 地址、连续地址段、网段、URL 等实时远程在线进行服务探测、存活性检测、应用指纹识别等工作，同时，支持 URL 资产快速发现；

系统漏洞扫描，包括：操作系统、网络设备、数据库、中间件等漏洞扫描，此外还可以选择紧急漏洞进行单独评估，实现紧急漏洞批量排查；

Web 漏洞扫描，包括：SQL 注入、XSS、敏感信息泄露等 OWASP TOP 10 应用漏洞扫描，此外还可以选择紧急漏洞进行单独评估，如 JBoss 反序列化漏洞、Apache Struts2 远程代码执行系列漏洞、Weblogic 反序列化专项漏洞、Jenkins Java 反序列化远程代码执行漏洞；

基线配置核查支持对常见的操作系统、数据库、中间件等系统配置核查，可根据等级保护二级、三级标准配置基线扫描及核查，做差距评估分析，基线核查支持在线基线配置核查和离线基线核查；

系统服务支持诊断日志Debug模式；诊断日志包括WEB日志、后台日志、关键日志；并提供专家诊断接口，提供界面截图证明。

web防扫描工具要求

工具具备独立的 WEB 应用防护识别库，特征总数在 3500 条以上；（需提供相关功能截图证明）

支持抵御 SQL 注入、XSS 攻击、网页木马、网站扫描、WEBSHELL、跨站请求伪造、系统命令注入、文件包含攻击、目录遍历攻击、信息泄露攻击、WEB 整站系统漏洞等攻击；（需提供相关功能截图证明）

支持对 Web 漏洞攻击防护；

支持对常见应用服务（HTTP、FTP、SSH、SMTP、IMAP、POP3、 RDP、Rlogin、SMB、Telnet、Weblogic、VNC）和数据库软件（MySQL、Oracle、MSSQL）的口令暴力破解防护功能；

支持 HTTP 协议异常检测，包括 HTTP 请求异常检测、HTTP 头部字段 SQL 注入检测、URL 溢出检测、Post 实体溢出检测、HTTP 头部溢出检测；（需提供相关功能截图证明）

支持 FTP 弱口令检测、WEB 登陆弱口令检测、WEB 登陆明文检测、口令暴力破解防护；（需提供相关功能截图证明）

支持 CC 攻击、CSRF 攻击、COOKIE 攻击等攻击防护功能；

支持针对网站的漏洞恶意扫描进行防护，能够拦截漏洞扫描设备或软件对网站漏洞的扫描探测，支持基于目录访问频率和敏感文件扫描等恶意扫描行为进行防护；（需提供相关功能截图证明）

支持应用隐藏，可替换服务器和请求出错页面；

支持对 SSL 解密，可对 HTTPS 加密会话进行分析；

支持 Web 漏洞扫描功能，可扫描检测网站是否存在 SQL 注入、CSRF、XSS、远程文件包含、DOM 跨站脚本攻击等漏洞；（需提供相关功能截图证明）

支持业务模型学习监督功能，通过智能分析引擎对业务流量进行分析学习，建立用户业务特征模型，解决因 WEB 应用中因代码不规范和安全检测功能冲突导致的业务误判问题；（需提供相关功能截图证明）

设备提供 URL 访问控制功能，能够基于多种 HTTP 方法执行访问控制，包括：GET、POST、UNKNOWN、HEAD、PUT、DELETE、MKCOL、COPY、MOVE、OPTIONS、PROPFIND、PROPPATCH、LOCK、UNLOCK TRACE、SEARCH、CONNECT，提供配置界面截图盖章证明。

设备支持通过获取爬虫程序代理列表跟进代理列表中包括多种爬虫程序；获取所述爬虫程序代理列表中各爬虫程序的性能加权值；根据各爬虫程序的性能加权值，确定目标爬虫程序；从而能够根据不断出现的钓鱼网站适应调整。(提供国家权威部门对技术的鉴定结果证明资料，并提供相应材料的网站链接和截图。)

支持Cookie安全机制，包括加密和签名的防护方法，支持Cookie自学习，提供配置界面截图盖章证明。

支持 SQL 注入、XSS 防护，支持使 HTTP 头域中的 Cookie、Referer、User-Agent，Except 字段过防护策略，提供配置界面截图盖章证明。

六、评分标准

评分权重：

项目	商务	技术	价格
分值	30 分	50 分	20 分

6.1 商务评分表

评审内容	评分细则	分值	实际得分
1、公司资质	1）具备中国网络安全审查技术与认证中心 CCRC 风险评估资质，提供证书复印件，具备得 3 分，无或其他 0 分； 具备中国网络安全审查技术与认证中心 CCRC 安全运维资质或应急处理资质，提供证书复印件，具备得 3 分，其他 0 分； 具备质量管理体系认证证书，提供证书复印件，具备得 3 分，其他 0 分； 持有广东省网络安全应急响应平台 2018 年技术支撑单位证书，具备得 3 分，无或其他 0 分；	12	
	3）近两年来参与省级范围（或全国范围）重大安全保障工作，提供相关证明。每提供一项，得 2 分；满分 4 分；其他或无不得分。	4	
	4）具备有效的 ISO9001 质量管理体系认证证书、信息安全管理体系认证证书，广东省计算机信息系统安全服务备案证，每提从一项，得 2 分，满分得 6 分；其他或无不得分。	6	
2、同类项目业绩	提供 2015 年以来（以合同生效时间为准）的同类（网络信息安全服务）项目（单项 20 万元或以上）业绩，每提供一个合同复印件得 2 分，满分 8 分。	8	

6.2 技术评分表

评审内容	评分细则	分值	实际得分
1、总体设计及响应程度	2.对项目整体需求的理解，技术方案整体思路明确清晰，是否全部囊括采购人要求的各项内容： 优秀（10～8 分）：整体服务方案优于招标文件要求，整体思路明确清晰；良好（7～5 分）：整体服务方案基本符合招标文件要求，整体思路较清晰； 尚可（0-4 分）：整体服务方案与符合招标文件要求有差距，思路较清晰；	10	

2、项目经理资质	为保障项目服务质量和实施进度，服务商的项目经理需同时具备以下证书：CCIE、PMP、CISSP、CISA 得 10 分，一项不满足扣 2.5 分，扣完为止。	10	
3、安全服务工具优异性评价	漏洞扫描工具全部满足得 15 分，每一项不满足扣 5 分，扣完为止	15	
	web 防扫描工具全部满足得 15 分，每一项不满足扣 5 分，扣完为止	15	

6.3 价格评分表

评审内容	评分细则	分值	实际得分
报价	项目投标报价得分（各有效投标投标人的投标报价中，取最低者作为基准价，各有效投标投标人的价格评分统一按照下列公式计算：价格评分＝（基准价÷投标人报价）×20）。	20	

七、付款方式

本项目使用财政资金，支付方式与进度以单位最终财政预算列支情况为准。