编制人	
审阅人	
批准人	

山东省医疗保障局网络信息和数据安全监管服务项目竞争性磋商文件

（本项目为预采购，有取消和终止采购的可能，供应商应充分考虑此风险之后决定是否参与投标）

项目编号：SDGP370000000202302009601

（SDHH-SDCS-231102）

采 购 人：山东省医疗保障局

代理单位：山东海恒项目管理有限公司

日　　期：2023 年 11 月

第三部分　项目说明及要求

一、建设背景

山东省医疗保障局高度重视本省医疗保障信息化的网络和数据安全工作，按照国家局相关文件要求，在现有网络安全、数据安全建设的基础上，开展网络安全及数据安全相关专项服务工作，补齐安全短板问题，夯实自身网络与数据安全检测防护能力，确保全省医保信息平台安全平稳高效运行。

二、服务目标

通过本次安全服务，不断健全本省医疗保障系统网络安全和数据安全保护制度体系，通过安全咨询、安全测试、安全评估、安全运营、安全预警、攻防演练、安全培训等服务，使智慧医保工作达到新水平。

1、建立采购人网络安全应急工作机制，发现存在的潜在威胁与漏洞，提升全员安全意识，提高应对网络安全的技术能力、预警能力及突发隐患应急响应能力。

2、以系统数据安全保障为业务目标，全面建立数据安全管理制度，落实分级分类管理及重要数据保护目录，实现数据全生命周期安全管理，明确数据共享使用流程，提升医疗保障数字化、智能化水平。

三、服务内容

1、网络安全专项服务

该专项服务包含了安全漏洞治理专项服务、网络安全运营专项服务、重大活动保障和攻防演练专项服务，具体服务内容如下：

（1）定期业务系统渗透测试

供应商需通过专业的渗透测试工具，利用人工渗透测试，模拟黑客攻击等相关手段，周期性评估山东省医疗保障局资产面临的威胁以及威胁利用脆弱性导致安全隐患的可能性，并结合渗透测试结果与所涉及的资产价值来判断安全隐患一旦发生对组织造成的影响。在威胁漏洞被整改之后，对系统进行复测，确保漏洞已被修复。

（2）新上线业务系统安全检查

供应商提供新业务上线安全检查服务，要综合采用访谈、漏洞扫描、渗透测试、代码审计、安全配置检查、后门检查等方法对新上线业务进行安全检查，山东省医疗保障局新业务上线前通知供应商提供新业务上 线安全检测服务，供应商在规定时间内完成测试环境的安全检测，

并提供检测报告，对发现的漏洞提出详尽的整改建议。在漏洞整改完毕后，对系统进行复测，确保漏洞已被修复。

（3）最新漏洞预警响应服务

供应商服务期内提供全年度的最新漏洞预警响应服务，该服务要求针对山东省医疗保障局业务系统涉及的各供应商产品、设备的安全漏洞，第一时间将通告信息以多种方式告知山东省医疗保障局相关人员，对于特殊突发情况，同时提供紧急安全通告，保障山东省医疗保障局能够第一时间了解、掌握最新安全风险。通告信息中应包含：官方提供的漏洞解决方案，若官方尚未给出解决方案的漏洞，则需要供应商技术专家团队给出临时性解决建议，确保信息权威、准确。对被整改过的漏洞进行复测，确保漏洞已被修复。

（4）安全加固支撑服务

服务期内对山东省医疗保障局业务系统涉及的主机、网络设备、数据库、安全设备、中间件提供安全加固协助支撑服务，供应商工程师利用服务工具及现网中的安全设备，有针对性结合安全漏洞实际情况提供整改建议，同时对发生的安全隐患进行处置与防御策略配置的优化，提高系统抵御外来入侵攻击的能力，缩小影响范围，使业务系统可以长期保持在高度可信的状态。

（5）互联网攻击面管理服务

通过供应商自身的情报数据、攻防战队、运营专家等安全能力，结合山东省医疗保障局实际情况，对山东省医疗保障局在互联网侧提供服务的资产、系统进行持续的监控，分析可能被攻击者利用的风险及攻击路径，辅助山东省医疗保障局采取措施闭环处置，持续提高安全能力。

（6）全天候威胁监测分析研判服务

提供 5 x 8 小时现场服务，7x24 小时云端威胁监测服务，通过对事件实时预警、失陷主机应急响应清理、失陷原因溯源等手段，实现失陷主机的自动化持续跟踪，确保恶意程序和各种权限维持手段得到完全清理。

（7）网络安全应急演练服务

服务期间，提供 1 次应急演练服务。安全应急演练服务的对象范围主要针对山东省医疗保障局核心业务及支撑核心业务的资源、人员、组织、流程、场所等，通过开展应急演练，查找已经编制的应急预案中存在的问题，进而完善应急预案，同时检查应对突发隐患所需应急队伍、物资、装备、技术等方面的准备情况，发现不足及时予以调整补充，做好应急准备工作。

（8）攻防演练服务

服务期间，组织 1 次现网实地攻防演练服务，同时承担活动组织和相关攻击队协调的协调工作，选取我省市各单位业务系统作为靶标系统，我省市各单位作为防守方，依托现有的安全检测和防护手段对攻击队的行为进行检测分析研判处置，提升采购人网络安全防护体系的实时监测、通报预警、应急处置能力和安全防护水平。

（9）重大活动保障服务

在重大活动安保期间，提供 7×24 小时现场监测与应急响应服务，包含护网期、大型赛会、重大节假日等，同时需至少加派一名高级安全工程师赴现场参与保障活动，从而保证整个网络的安全性。

（10）网络安全意识培训服务

服务期间提供 1 次的网络安全意识培训服务服，加强工作人员信息安全意识，了解当前信息安全技术的发展状况，建立信息安全的敏感意识和正确认识，增强安全意识防护能力，有力保障采购人的信息安全。

2、数据安全专项服务

数据安全专项服务旨在通过完善的数据安全制度体系建设、技术体系建设、运营体系建设，有效支撑山东省医疗保障局数字化改革全周期。通过引入国际先进技术体系、管理标准，以 ISO27001、等保三级为建设基准，打造立体、纵深、可追溯的数据安全防控系统，形成安全、合规、全面、稳定、高效的数据安全架构，构建纵横防御数据安全架构体系。

数据安全管理制度体系:建立健全数据安全制度规范体系，制定完善数据分类分级、访问权限、共享开放、脱敏销毁、供应链安全、日志审计、监督检查、安全隐患应急处置等标准规范，促进数据安全管理工作标准化、流程化、规范化，使数据安全管理各项工作有规可依。

数据安全技术防护体系:以数据分类分级为基础，明确数据全生命周期各环节的安全防护要求。通过态势感知、权限管控、数据脱敏、高危操作阻断、数据水印溯源、日志审计等安全技术手段，加强数据安全常态化监测和智能风险预警，全面提升数据安全防护，筑牢数据安全防线。

数据安全运营服务体系：结合数据安全管理制度体系要求，充分利用数据安全防护技术工具，完善数据安全风险识别、安全防御、安全检测、安全响应和安全恢复管理手段，提升数据安全运行保障，建立事前管审批、事中全留痕、事后可追溯的全链路数据安全监管机制，及时发现处置各类数据安全风险，切实防范数据篡改、泄漏、滥用。

通过三大体系的建设，结合医保行业要求、山东省医疗保障局现状，要求综合调研数据安

全业务现状，锚定重要业务系统，识别从数据采集、传输、存储、处理、交换、销毁全生命周期各环节风险点。锚定重点业务场景，针对第三方运维、开发、测试等场景重点评估，识别数据安全风险。

具体服务内容如下：

（1）数据安全咨询服务

数据安全咨询服务包括制定数据安全战略目标，构建数据安全体系框架和能力评估模型、开展数据安全现状调研、差距分析、安全架构设计、数据安全建设规划蓝图设计、确定任务实施路线图、保障措施等内容。

通过梳理国家政策指引、行业发展动态、监管指引方向，明确合规需求；综合分析数据安全能力成熟度评估报告与数据安全风险评估报告中呈现的数据安全能力弱点，基于风险视角量化分析山东省医疗保障局数据安全建设需求；在设计规划蓝图阶段，参考行业内需求与行业最佳实践，选取调整符合行内现状的建设方法论，基于建设目标设计行内数据安全能力建设框架。根据风险紧迫程度、任务投资和实施的难易程度、任务建设实施的预期效果、任务运维管理成本等四方面量化评估分析，确定任务实施的优先级，规划建设蓝图，制定建设实施计划。

（2）数据安全管理体系建设服务

结合山东省医疗保障局现状，对标《中华人民共和国数据安全法》、《中华人民共和国个人信息保护法》等相关法律法规要求，对数据安全管理制度体系查缺补漏，充分考虑可执行性，重点聚焦在数据分类分级、访问权限、共享开放、脱敏销毁、供应链安全、日志审计、监督检查、安全隐患应急处置等标准规范，补充具体指导性操作。同时完善重要业务场景流程标准，如取数、内外部共享过程、第三方运维开发管理等具体管理要求。

（3）数据资产分类分级服务

参照国家医疗保障局《医疗保障信息系统数据分类分级规范》（修订版）、《山东省健康医疗大数据管理办法》以及山东省医疗保障局业务需求，通过专业的工具，理清数据资产，实现对数据资产的动态维护，并对数据资产进行分类分级的标识，完成打标识后，明确数据分级防护策略，让数据使用者明确所使用数据的安全等级，并对照相应策略要求，针对性建设数据安全能力；同时，分类分级结果可以同其他数据安全保护工具（如脱敏平台、水印工具）联动，对敏感数据做到精准保护，为各类场景下的数据安全管控措施采用提供指导和依据，在确保安全的前提下促进数据开发利用，降低安全防护成本。

（4）数据安全风险评估服务

依据有关数据安全技术与管理标准，结合山东省医疗保障局现状，从组织人员建设、制度流程、技术措施三个维度，对数据全生命周期接触个人信息、重要数据的人员行为审查机制，数据安全领域的制度规范和流程落地建设情况，采取安全技术措施包括身份认证和授权访问机制和技术工具、访问控制机制和实现方式、安全审计和数据溯源机制方法、数据加密和泄露防护措施等开展全面的安全评估，校验控制措施的有效性。

服务人员通过调研访谈等形式，对数据流转过程中面临的数据威胁进行分析确认，结合数据、流程、用户、环境等要素，以敏感数据为中心，从技术角度识别评估敏感数据在业务流程中的威胁风险点，明确敏感数据泄露的可能途径，通过梳理威胁信息并结合威胁调查判定的威胁源发生的频率和可能性，对威胁进行评估并赋值。

（5）数据流转脱敏服务

山东省医疗保障局数据涉及大量的个人隐私数据，在与其他单位进行数据交互的过程中，就极有可能造成数据的泄露，因此需要对外发的数据进行规范化、流程化的脱敏，防止出域数据携带有敏感信息，从而造成敏感信息的泄露，提高数据安全性。

需对指定的系统内置敏感数据特征或自定义的敏感数据特征，在敏感数据发现任务中对抽取的数据进行自动识别敏感数据，配合定时增量敏感数据发现任务，可持续自动发现新的敏感数据。

（6）数据安全运营服务

以数据安全合规为目标，以数据资产为核心，结合数据安全运营平台，汇聚全网数据安全日志数据，建立重要数据访问行为基线，帮助山东省医疗保障局从海量数据访问中准确识别数据访问行为异常和数据泄露风险，并提供风险隐患闭环管理机制，提升数据安全风险监控能力，降低风险导致的损失，同时呈现全网数据安全综合态势，基于上传下达通道拉通不同部门参与数据安全工作，提升数据安全运营能力。

（7）数据安全培训服务

根据《中华人民共和国数据安全法》和《信息安全技术个人信息安全规范》，结合供应商自身能力，对山东省医疗保障局相关人员提供数据安全培训服务，通过知识（Knowledge）、能力（Ability）、技能（Skill）的传授，帮助山东省医疗保障局人员构建正确的数据安全知识框架，掌握数据安全治理工作的核心能力，并在模拟实践中习得实际工作环境中所需的技能，使山东省医疗保障局人员具备开展数据安全治理工作所需的能力。

四、服务要求

（一）服务交付要求

供应商应按照项目工期要求，提供切实可行的项目实施方案，制定项目进度计划表。

服务期限为：自合同签订之日起一年。服务交付地点：由采购人指定地点。

（二）服务工具要求

本次服务项目中，所涉及服务工具全部由供应商负责提供，供应商必须保证服务工具自主研发、安全可靠，且服务工具需为国产化信创产品或支持在信创环境中部署，工具至少要具备以下要求：

1、网络安全专项服务

为保障系统的可用性及服务的质量，供应商应在服务过程中提供专业的服务工具，工具至少满足以下要求：

- 网络安全运营管理平台

△平台需支持多种设备日志解析规则查看以及筛选，包括但不限于网络设备（防火墙、交换机、网关）、安全设备（入侵检测设备、WEB 攻击防护设备、APT 检测设备、防火墙、网络审计、流量探针等）、Linux 主机日志、数据库等。

平台需支持对失陷资产进行判定并提供失陷资产的判定依据，包括但不限于失陷资产概要信息、攻击结果、攻击链分布阶段、失陷资产的攻击过程及过程判定依据如攻击特征、流量上下文、关联的告警日志及流量日志以及 pcap 包下载，并可快速扩展该失陷资产的全部攻击事件以及该失陷资产攻击者发起的攻击、该失陷资产的同类型威胁事件。

△平台需支持对重点网站的漏洞扫描能力，可统一下发系统漏洞扫描任务、网站安全漏洞扫描任务、口令猜测扫描任务，通过平台进行统一扫描任务监控、管理，对扫描结果可以进行可视化呈现。

平台需支持漏洞分析能力，可基于资产视角浏览不同资产上的漏洞分布情况，描述资产风险并统计不同资产上发生不同危险等级的漏洞数量，也可通过漏洞视角浏览漏洞在不同资产上的分布情况，监测该漏洞发生的次数和出现在资产上的情况等。

△平台需支持内置策略结合策略配置的方式对安全隐患进行自动化响应以提升响应效率和响应精准度，支持数据源、研判取证、响应等流程，支持精确模式和模糊模式的数据来源。

供应商需具备自建的威胁情报中心，平台可接入威胁情报中心，将本地告警数据、网络资

产数据、漏洞数据与威胁情报中心按照多个维度进行关联分析，实时感知资产的威胁和脆弱性，通过平台安全规则的筛选和过滤最终形成漏斗效应，保证告警的更加精准和有效，并洞察新的威胁动向，了解最新的威胁动态，实施积极主动的威胁防御和快速响应策略，提前预防 0day 漏洞和重大攻击的发生，减少安全损失。

平台应为被广泛应用的成熟产品，具备由中国信息安全测评中心颁发的国家信息安全测评信息技术产品安全测评证书 EAL3+和国家信息安全漏洞库兼容性资质证书。

- 漏洞扫描工具

△工具需支持扫描国产操作系统、应用及软件的安全漏洞，要求能够扫描相关漏洞。

工具需支持对 C/C++/Python/Java/Php/go 等语言的代码解析，语言的词法、语法分析，内置缺陷模板和缺陷规则，并支持自定义。

工具需支持单独口令猜测扫描任务，支持多种口令猜测方式，包括利用 SMB、RDP、SSH、Telnet、SQL SERVER、MySQL 、Oracle、Sybase、DB2、MongoDB、Memcached、Redis 、PostgreSQL 、HighGo 、UXDB 、Kingbase 、STDB 、FTP、SFTP、ActiveMQ、POP3、Tomcat、SMTP、IMAP、Onvif、RTSP、 SNMP、SIP、Vmware ESXi、HTTP Digest、Weblogic、Elasticsearch、Websphere 等协议进行口令猜测，允许外挂用户提供的用户名字典、密码字典和用户名密码组合字典。

工具需支持扫描主流云主机管理系统、云计算组件的安全漏洞。

△工具需支持对扫描出的漏洞提供取证性质的验证并输出报告，直观展示漏洞利用过程和危害性。支持漏洞验证扫描任务，包括系统漏洞验证扫描、Web 漏洞验证扫描。

2、数据安全专项服务

为保证数据安全专项服务质量，供应商应在服务过程中提供专业的服务工具，工具至少满足以下要求：

- 数据分类分级工具

工具应具备用自动化的数据分类分级，同时根据采购人的业务数据特性，提供数据分类分级模板，便于使用；可自定义规则，根据采购人自身业务特性，可自定义数据分类分级规则和模板。

工具应具备对静态存储在传统关系型数据库和分布式数据库中的结构化数据、半结构化数据、非结构化数据进行主动扫描，对扫描出的数据资产进行识别、分类、分级、存储位置记录，以数据库、数据表、数据字段、簇/列的维度，对数据资产做统计分析，梳理出数据资产全景图。

● 数据流转脱敏工具

△工具应为被广泛应用的成熟产品，具备中国网络安全审查技术与认证中心颁发的《IT产品信息安全认证证书》。

△工具应具备丰富的脱敏算法，至少具备同态加密算法、差分隐私算法等，可根据采购人实际情况灵活选择不同的算法进行脱敏。

工具需支持对Oracle、SQLServer、MySQL 、DB2 、PG、KingBase、Gbase 8a/8s、Hive、DM、SAP HANA、Cache、Gauss DB-A/T、ES、MongoDB、OceanBase、GrennPlum、HBase、IRIS、enterprisedb、MariaDB、TiDB、TXT、CSV、XLSX、XLS、Oracle DMP、DICOM、HDFS、XML、JSON等常见数据源的脱敏。

工具应具备API的自动收集及API脱敏功能。

● 数据安全运营平台

平台需支持数据资产管理、数据安全隐患、数据安全合规相关页面分权分域功能，管理员可以看到组织数据，具体分子账号看到自己数据。

△平台需支持数据安全隐患列表，可对数据安全隐患进行滚动播放，包括事件名称、事件类型、发生时间、源IP、目的IP、业务系统、部门/单位、风险等级。不同账号可以看到自己资产对应的数据安全隐患。

平台需支持对数据安全隐患进行详情查看、研判、分配资产、下发处置、完成处置、审核、下载报告操作。支持批量操作，支持数据安全隐患清单导出功能。

△平台需支持字段粒度相关数据库信息展示：支持以字段粒度展示数据库对应的类别、一级子类、二级子类、数据级别、数据表、数据库、业务系统、部门/单位、变更类型、稽核状态、变更原因、变更时间。

平台需支持对流转中的数据进行监控，自动化发现并测绘出重要业务系统的重要或敏感数据的流转链路视图，并基于该流转链路视图，对高敏数据传输风险进行针对性聚焦。

△平台需支持以列表方式展示所选时间范围内新增、变更及全部三个维度的数据库/文件资产分类分级分布统计TOP。拖动鼠标或单击数据级别图标，可以通过数据级别进行筛选。

△平台需支持数据安全隐患处置功能，可针对数据安全隐患进行详情查看、研判、分配资产、下发处置、完成处置、审核、下载报告操作，对于已经进行资产管理的数据安全隐患，点击下发处置，无需选择人员，对于事件未关联到资产，可以点击分配按钮，将事件指派至对应的责任人；也可以发起资产认领工单，让全部人员按需认领相关数据资产，完成事件与资产打

标。

所有带“△”项为重要指标项，须提供相关功能证明材料并加盖公章。

（三）服务管理要求

供应商须提供完整的服务管理方案，包括服务计划、组织架构、进度控制、质量管控、风险管理方案。

（四）服务人员要求

本次服务项目分为网络安全专项服务和数据安全专项服务，对于服务人员要求如下：

在服务期内，供应商所安排的驻场人员需要专职于本项目的建设，项目经理和服务交付的主要人员未经采购人同意不得调整；供应商如中途更换项目经理和主要服务人员，必须提前提出书面申请，经按规定标准考核合格、经采购人认可后并进行过一定的适应性服务工作方可完成替换。

本次服务的项目经理应为供应商正式员工。

（1）网络安全专项服务

为保证服务质量，供应商应成立专业的网络安全运维团队，成员应不少于：1 名驻场场工程师、3 名服务实施工程师、3 名安全研究专家。团队成员需满足以下要求：

1、 驻场工程师需提供 5*8 小时驻场服务，如遇重大活动需提供 7*24 小时值班随客户工作时间进行安排。

2、驻场工程师需具备相关行业运维工作经验，需熟悉本次服务其提供的威胁分析平台工具，并同时可基于平台开展告警监测、漏洞通告及整改跟踪、安全咨询支持和安全运行情况统计分析工作。

（2）数据安全专项服务

为保证服务质量，供应商应成立专业的数据安全运维服务团队，团队成员应不少于：1 名驻场工程师，3 名的服务实施工程师，3 名的安全专家，团队成员需满足以下要求：

1、驻场工程师需具备相关行业运维工作经验。

2、驻场工程师可利用熟练运用数据安全运营平台，将不同孤立的安全设备信息汇聚融合分析，实时监控采购人数据安全风险态势，提供数据流转监控、数据资产梳理、数据安全风险监控、数据安全策略管控、数据安全隐患溯源、数据安全风险告警等功能。

需提供以上人员近 6 个月内任意 1 个月在本单位的社保缴纳证明复印件。

（五）服务响应要求

（1）服务期内，供应商应提供 7X24 小时的服务响应，当采购人提出响应需求时，供应商需指定专门的工程师负责处理，并进行处理过程的全程跟踪，保障后续的事件升级工作，工程师应在 0.5 小时内做出响应并立即提供在线技术支持，在 2 小时内抵达现场进行技术支持。

（2）服务期内，除驻场服务外，供应商还应提供多种服务方式，包括但不限于：现场服务、电话服务、远程服务、邮件服务等.

（3）服务期内，所有服务方式产生的一切服务费用，均需有供应商承担。

（六）项目验收要求

服务期满，供应商应按照项目合同完成服务，并已经进行了必要的各个阶段的验证、确认、评审，在服务期内按要求持续提供优化升级服务，具备完整的项目验收文档，由山东省医疗保障局组织验。项目验收应当遵循的基本程序包括：制定项目验收办法，编写项目验收报告等工作。验收组对服务内容与实施服务情况进行检验，要求包括但不限于如下：

（1）实现合同和采购、响应文件中列举的全部服务要求。

（2）文档齐全，符合合同和采购、响应文件及国家医疗保障局、省大数据局相关最新标准要求。

（3）验收项目包括按照合同和采购、响应文件中所标明的服务内容及相关的技术维护文档、培训教材、使用说明书等。

（七）培训要求

针对网络安全服务专项、数据安全服务专项，提供相应的安全培训服务。

（1）对于所有培训，供应商必须派出具有相应专业资格和实际工作经验的辅导人员进行培训。

（2）成交供应商负责师资及教材，须提供详细的培训计划、方案，制定详细的人员培训方案，包括培训目的、培训方式、培训内容、培训课程、培训计划等，并负责对培训过程及效果进行跟踪、评估、记录，形成有效项目培训记录资料。供应商必须派出具实际工作经验的教师及辅导人员进行培训。

（3）培训费用由成交供应商承担。

第四部分 政府采购政策

一、中小企业优惠办法：

1.根据（财库〔2020〕46 号）《政府采购促进中小企业发展管理办法》、（鲁财采〔2022〕12 号）《关于落实政府采购支持中小企业发展有关政策措施》的通知，专门面向中小企业的采购项目或采购包，不享受价格评审优惠，对于经主管预算单位统筹后未预留份额专门面向中小企业采购的采购项目，以及预留份额项目中的非预留部分采购包，对符合本办法规定的小型和微型企业价格给予（货物和服务项目为 10%、工程项目为 5%）的扣除，用扣除后的价格参与价格得分的计算及评审；

小型、微型企业提供中型企业制造的货物的，不享受价格优惠评审。

2.小微企业评标价格的计算：

服务项目若所投企业为小微企业的，则最终评审价格=投标报价×（1-10%）。

货物项目若所投全部产品为小微企业的，则最终评审价格=投标报价×（1-10%），依据《管理办法》第四条 在货物采购项目中，供应商提供的货物既有中小企业制造货物，也有大型企业制造货物的，不享受本办法规定的中小企业扶持政策。由此可知，当供应商所投部分产品为小微，其他为大型企业制造的，不作价格扣除。

工程项目若所投企业为小微企业的，则最终评审价格=投标报价×（1-5%）。

3.如供应商为小微企业，应根据工业和信息化部、国家统计局、国家发展改革委、**财政部《关于印发中小企业划型标准规定的通知》（工信部联企业〔2011〕300 号）**，结合本公司实际情况如实填写中小企业声明函（格式见附件），否则不给予价格扣除；未按要求提供声明函原件的，或者经审查不符合中小企业划型标准的，将不给予价格扣除的政策优惠；

4.联合体投标的，如果联合体由大中型企业与小型、微型企业组成，且组成联合体的大中型企业与小型、微型企业之间不存在投资关系，联合投标协议中约定，小型、微型企业的协议合同金额占到联合体协议合同总金额 30%以上的，则在评审过程中评标价格可给予联合体（货物和服务项目为 4%、工程项目为 2%）的价格扣除。如果联合体各方均为小型、微型企业的，联合体视同为小型、微型企业，则在评审过程中评标价格可给予联合体 10%的价格扣除，但联合体各方均应按规定提供中小企业声明函原件。

货物和服务项目计算方法是：最终评审价格＝投标报价×（1-4%），按照最终价格计算其价格。

工程项目计算方法是：最终评审价格＝投标报价×（1-2%），按照最终价格计算其价格。

执行政府采购政策对投标报价进行扣除后的评标价格仅用于评标过程的报价得分计算或评标价格的比较，不作为最终的中标价格。

二、 政府采购支持监狱企业发展的政策：

1.按照《财政部 司法部关于政府采购支持监狱企业发展有关问题的通知》（财库【2014】68 号）文件规定，在政府采购活动中，监狱企业视同小型、微型企业，享受评审中价格扣除的政府采购政策。

2.参加政府采购活动的监狱企业应当在响应文件中提供监狱企业证明复印件，否则不予认定。监狱企业证明须由省级以上监狱管理局、戒毒管理局（含新疆生产建设兵团）出具。

三、残疾人福利性单位优惠办法：

1.按照《财政部 民政部 中国残疾人联合会关于促进残疾人就业政府采购政策的通知》（财库【2017】141 号）文件规定，在政府采购活动中，残疾人福利性单位视同小型、微型企业，享受预留份额，评审中价格扣除等促进中小企业发展的政府采购政策。

2.供应商为残疾人福利性单位或提供其他残疾人福利性单位制造的货物（不包括使用非残疾人福利性单位注册商标的货物）的，涉及部分价格将做扣除，须提供《残疾人福利性单位声明函》（后附）并满足以下条件：

2.1 安置的残疾人占本单位在职职工人数的比例不低于 25%（含 25%），并且安置的残疾人人数不少于 10 人（含 10 人）；

2.2 依法与安置的每位残疾人签订了一年以上（含一年）的劳动合同或服务协议；

2.3 为安置的每位残疾人按月足额缴纳了基本养老保险、基本医疗保险、失业保险、工伤保险和生育保险等社会保险费；

2.4 通过银行等金融机构向安置的每位残疾人，按月支付了不低于单位所在区县适用的经省级人民政府批准的月最低工资标准的工资；

2.5 提供本单位制造的货物、承担的工程或者服务（以下简称产品），或者提供其他残疾人福利性单位制造的货物（不包括使用非残疾人福利性单位注册商标的货物）。

前款所称残疾人是指法定劳动年龄内，持有《中华人民共和国残疾人证》或者《中华人民共和国残疾军人证（1 至 8 级）》的自然人，包括具有劳动条件和劳动意愿的精神残疾人。在职职工人数是指与残疾人福利性单位建立劳动关系并依法签订劳动合同或者服务协议的雇员人数。

注：同时属于小型、微型企业、监狱企业和残疾人福利性单位的，不重复享受价格扣除政策。

四、节能、环保产品优惠办法：

1.节能产品是指列入财政部、国家发展和改革委员会制定的《节能产品政府采购清单》，且经过认定的节能产品。环境标志产品是指财政部、国家环保总局制定的《环境标志产品政府采购清单》，且经过认证的环境标志产品。

2.属于政府强制采购节能产品的，必须按照强制采购节能产品清单填报，对采购非政府强制采购节能产品而提供节能产品的须单独分包列明 （报价表格式见附件）。

3.根据《山东省节能环保产品政府采购评审办法》（鲁财库〔2007〕32 号）的规定，采用综合评分法评标时，在满足基本技术条件的前提下，在价格评标项中，对节能、环保产品分别给予价格评标总分值、技术评标总分值的 5%的加分：

3.1 在投标报价打分中，投标设备属于节能、环保产品的：若所投全部产品为节能、环保产品，在其价格评标总分值基础上给予（价格评标总分值×5%）的加分，若所投部分产品为节能、 环保产品，在其价格评标总分值基础上分别给予[价格评标总分值×5%×（节能、环保产品合计报价/投标报价）]的加分。

3.2 在技术部分打分中，投标设备属于节能、环保产品的：若所投全部产品为节能、环保产品，在其技术评标总分值基础上分别给予（技术评标总分值×5%）的加分，若所投部分产品为节能、环保产品，在其技术评标总分值基础上分别给予[技术评标总分值×5%×（节能、环保产品合计报价/投标报价）]的加分。

3.3.采用最低评标价法评标时，在评审时可以对节能、环保产品分别给予 5%的价格扣除。

3.4 供应商所投产品如属节能环保的产品，应在响应文件列明某项/某些产品属于节能环保产品，并列明节能环保产品的生产厂家及产品品牌、型号、节能或环保标志认证证书编号（有效期内）等，并后附有效的国家节能产品认证证书和中国环境标志产品认证证书（复印件加盖公章），否则将不给予价格扣除的政策优惠（格式详见附件）。