德清县公安局
首届联合国世界地理信息大会官网安全防护项目

德财采确临[2018]4705号

竞
争
性
磋
商
文
件

项目编号：DQZCFW-2018-JC104

德清天勤会计师事务所有限责任公司

2018年11月2日

目　录

第一章　采购公告
第二章　竞争性磋商须知
第三章　采购内容及技术要求
第四章　磋商原则和程序
第五章　合同主要条款
第六章　采购响应文件格式

第一章 竞争性磋商公告

德清天勤会计师事务所有限责任公司受德清县公安局的委托，就其所需的首届联合国世界地理信息大会官网安全防护项目组织竞争性磋商采购。欢迎符合资格要求，能提供优质服务的供应商参加磋商。

一、 采购项目的名称、内容、用途：

1.项目名称：德清县公安局首届联合国世界地理信息大会官网安全防护项目

2.采购方式：竞争性磋商

3.采购编号：DQZCFW-2018-JC104

4.项目内容：

序号	采购内容	数量	预算（万）	采购单位
1	首届联合国世界地理信息大会官网安全防护	1 项	180	德清县公安局

详见第三章 采购内容及技术要求

二、 供应商资格要求：

A. 符合《中华人民共和国政府采购法》第二十二条的要求、财库【2016】125 号《关于在政府采购活动中查询及使用信用记录有关问题的通知》和浙财采监【2013】24 号《关于规范政府采购供应商资格设定及资格审查的通知》第六条规定；

B.拟磋商响应方必须是在中华人民共和国境内注册，且能提供本项目所要求货物及服务内容的供应商；（总公司所设立的区域性分支机构（分公司），以及个体工商户、个人独资企业、合伙企业，必须获得总公司（总机构）授权或能够提供房产权证或其他有效财产证明材料）

C.拟磋商响应方是在中国境内注册的企事业单位，须具有独立法人资格，且具有合法有效的法人营业执照；

C.本项目不允许转包或者分包；

D.本项目不接受联合体竞标。

三、 获取采购文件的时间、地点、方式及采购文件售价（在政采云进行网上报名的供应商需在采购响应截止时间前再向本代理机构另行提交一份书面报名资料）：

（凡政府采购注册供应商，均可通过浙江政府采购网，凭注册用户名和密码免费浏览或者下载本项目电子采购文件，电子采购文件与书面采购文件不一致时以书面采购文件为准。）

1.获取磋商文件时间：**2018 年 11 月 2 日**至 **2018 年 11 月 8 日**。上午 9：00～11：00 下午 14：00～16：30（节假日除外）。

磋商文件发售截止时间后至采购响应截止时间前允许潜在供应商前来认购磋商文件。但若磋商文件发售截止时间后认购磋商文件的供应商对本采购文件有异议，将不予受理、答复。

2.获取磋商文件地点：德清县武康街道永安街 272 号（德清天勤会计师事务所有限责

任公司)。

获取磋商文件方式：报名后现场领取。

售价：磋商文件工本费每套 500 元，售后不退。

报名时须提交以下文件资料，并满足本公告中对供应商的资格要求。

1)填写磋商报名登记表（现场领取并填写);

2)磋商单位的有效工商营业执照或法人证书复印件（加盖公章）**(磋商时原件备查)**

3)法定代表人授权书原件、授权代表身份证原件（查看）和复印件;

四、采购响应截止时间资格审查时应提供以下资料:【供应商是否具有竞标资格由采购单位或采购代理机构在磋商时审查，竞标截止时间止竞标供应商必须提供相应的竞标资格证明材料进行资格审查。资格审查时若需要供应商提供相应资格证明材料原件（公证件或经法定代表人签字并加盖公章的浙江省政府采购注册供应商证明材料等可替代相应原件进行备查）进行备查而供应商却无法提供的，其供应商的竞标文件将被作无效竞标处理。】

A.磋商响应方的有效工商营业执照或法人证书复印件加盖公章;（原件备查）

B.磋商响应方的依法缴纳税收(投标截止时间前近三个月缴纳增值税和企业所得税的完税凭据或税务部门出具的其他证明）和社会保障资金（投标截止时间前近三个月缴纳社会保险的凭证（专用收据或社会保险缴纳清单）或人社部门出具的其他证明）证明材料复印件加盖公章;（原件备查,依法免税或不需要缴纳社会保障资金的供应商，应提供相应文件证明其依法免税或不需要缴纳社会保障资金。）

C.供应商市场行为信誉（信用）情况承诺书原件（格式见附件，网站截图可由磋商响应方自行提供或磋商时由采购人或采购代理机构查询作为资格证明材料);

D.法定代表人授权书原件、授权代表身份证（原件查看）复印件一份;（磋商时，请另行准备一份法定代表人授权委托书原件及携带有效身份证明原件）

E.磋商响应方的其他资格证明文件复印件加盖公章(如果供应商为总公司所设立的区域性分支机构（分公司)，以及个体工商户、个人独资企业、合伙企业的，则必须提供此项；证明文件可以是房产权证、车辆行驶证或其他固定资产等有效财产证明材料复印件加盖公章)。(原件备查)

五、磋商答疑时间及现场勘查事项：

1、任何要求澄清或质疑采购文件内容的磋商响应方，均应在 2018 年 11 月 9 日（提交首次响应文件截止时间 3 日前）下午 16：00 前以书面（含传真）形式将需要澄清或质疑的事项向本代理机构一次性提出，本代理机构将在规定的时间内统一进行澄清和修改，并书面（含传真）通知所有认购采购文件的供应商，逾期未提出的，则视同认可采购文件，本代理机构将不予受理、答复。

2、本项目建议供应商报名完成后自行联系采购人进行现场考察,不进行集中考察。

六、磋商的时间及地点：

1.递交采购响应文件时间：2018 年 11 月 13 日，8:30～9:00（北京时间);

2.采购响应文件递交截止时间：2018 年 11 月 13 日，9:00 止（北京时间);

3.磋商时间：2018 年 11 月 13 日，9:00 正（北京时间);

4.采购响应文件递交及磋商地点：德清县武康街道永安街169号德清县公共资源交易中心二楼 201 磋商室；

5.经资格审查合格的报名供应商获取采购文件后，不得无故放弃磋商，确有特殊情况不能参加磋商的，应在磋商截止时间2天前以书面形式陈述原因，以（信函、传真加盖磋商单位公章）等方式通知本代理机构，如在规定期内未收到磋商响应方书面函件，则视为磋商响应方同意参加磋商。

七、磋商保证金：

1.磋商保证金的有关事项按采购文件中“竞争性磋商须知”的相关规定执行。

2.磋商保证金金额：人民币**18000元**(应备注本项目编号)

根据《政府采购货物和服务招竞标管理办法》相关规定，保证金必须在2018年11月12日上午9时前到达德清天勤会计师事务所有限责任公司的保证金帐户，否则其采购响应文件将被拒绝。保证金提交单位与报名单位必须主体一致。）

3.形　　式：以汇票、电汇或银行转帐等**非现金方式**；

4.单位名称：德清天勤会计师事务所有限责任公司；

5.开户银行：中信银行湖州德清支行；

6.银行帐号：8110801012800606483。

八、采购人、代理机构的名称、地址和联系方式：

1.采购人联系方式：

采购单位：德清县公安局

联系人：成女士　　联系电话：0572-8815098

地址：德清县宋石街108号

2.代理机构名称：德清天勤会计师事务所有限责任公司

代理机构地点：德清县武康街道永安街272号

代理机构联系人：陆长江（项目负责人）、刘钰滢

代理机构联系电话：0572-8061669　　传真：0572-8068141

3. 德清县财政局 联系电话：0572-8074859

九、本次采购项目相关信息发布媒体：

1.浙江省政府采购网：http://www.zjzfcg.gov.cn

2.德清县公共资源交易网：http://www.dqztb.gov.cn

十、质疑受理联系方式：

采购单位质疑受理人：成女士　　联系电话：0572-8815098

地址：德清县宋石街108号

代理机构质疑受理人：梁海芳　　联系电话：0572-8061669

地址：德清县武康街道永安街272号

请将质疑函以书面形式送达采购单位或采购代理机构。

十一、本磋商文件的解释权归招标采购单位所有。

德清天勤会计师事务所有限责任公司

2018年11月2日

第二章 竞争性磋商须知

序号	内容、要求
1	项目名称： 德清县公安局首届联合国世界地理信息大会官网安全防护项目
2	采购数量及单位：**详见第三章内容**
3	磋商报价及费用：1、本竞争性磋商项目报价以人民币为结算货币。 2、不论磋商结果如何，磋商响应方均应自行承担所有与磋商有关的全部费用。 **3、本次项目的代理费由中标供应商承担，按中标金额的相应比例收取，100 万元以下按 1.5%，100-500 万按 0.8%。**
4	保证金：参见竞争性磋商公告
5	答疑与澄清：如磋商响应方如认为采购文件表述不清晰、存在歧视性、排他性或者其他违法内容的，应当于 2018 年 11 月 9 日下午 16 点前，以书面形式要求招标采购单位作出书面解释、澄清或者向招标采购单位提出书面质疑**（逾期将不再受理）**，招标采购单位将做统一答复，如规定时间内未收到任何质疑，则视为各磋商响应方均对此无异议；招标采购单位将于提交响应截止时间 5 日前进行可能影响磋商文件编制的澄清或修改；澄清或修改内容是采购文件的组成部份，并将以书面形式送达所有已报名的磋商响应方。因其他紧急情况影响本项目正常磋商活动的，招标采购单位将于采购响应截止日期一天前书面通知所有已报名的磋商响应方。
6	采购响应文件组成：技术、资信商务和初次报价文件正本各1份，副本各2份**（不同标项响应文件应分开装订密封，未分开装订密封按无效标处理。）** **磋商最终报价应在磋商小组对技术、资信商务和初次报价文件评审完毕并在评分公布前提交。**
7	采购响应文件提交截止时间及地点：2018 年 11 月 13 日 9 时 00 分前德清县武康街道永安街 169 号德清县公共资源交易中心二楼 201 磋商室
8	磋商时间及地点：2018 年 11 月 13 日 9 时 00 分前 德清县武康街道永安街 169 号德清县公共资源交易中心二楼 201 磋商室
9	磋商的原则和程序详见采购文件第四章。
10	成交结果公示：磋商结束后，磋商结果公示于浙江省政府采购网(http://www.zjzfcg.gov.cn)、德清县公共资源交易网（http://www.dqztb.gov.cn）等网站或媒体。
11	成交公告及成交通知书：磋商结束后5个工作日内，成交公告发布于上述媒体。
12	保证金退还：除采购文件规定不予退还保证金的情形外，中标人签订合同后 5 个工作日内退还其投标保证金，其他磋商响应方的保证金在中标通知书签发后的 5 个工作日内按程序退还。
13	采购资金来源：预算内资金
14	服务时间：官网安全防护服务：自合同签订日起，持续两年； 大会期间重保服务：自合同签订日起，至 2018 年 12 月 31 日。

15	付款方式：待首届联合国世界地理信息大会重保服务完成且官网安全防护平台审核通过后，一次性付清。
16	采购响应文件有效期：90 日历天
17	**质疑：**根据《政府采购法》第五十二条的规定，供应商认为采购文件、采购过程和中标、成交结果使自己的权益受到损害的，可以在知道或者应知其权益受到损害之日起七个工作日内，以书面形式向采购人、采购代理机构提出质疑。同时，供应商须在法定质疑期内一次性提出针对同一采购程序环节的质疑。 （**质疑期限的计算**：（一）对采购文件提出质疑的，自供应商获得采购文件之日起计算，且应当在竞标截止之日或递交磋商、询价响应性文件截止之日前提出。（二）对采购过程提出质疑的，自采购程序环节结束之日起计算。（三）对中标、成交结果以及评标委员会、磋商小组、询价小组组成人员提出质疑的，自中标、成交结果公告之日起计算。）
18	**投诉：**根据《政府采购法》第五十五条的规定，质疑供应商对采购人、采购代理机构的答复不满意或者采购人、采购代理机构未在规定的时间内作出答复的，可以在答复期满后十五个工作日内向同级政府采购监督管理部门投诉。
19	**注意事项：**1、磋商响应方如发现采购文件及其评标办法中歧视性不公正条款或违法违规等内容时，请于答疑截止日期前同时向采购人、采购代理机构反映，逾期不得再对采购文件的条款提出质疑。 2、该项目中标公示期间，磋商响应方不得通过非正当途径、更不得通过非正当手段获取法律法规规定磋商小组（包括其他相关人员）应当保密的相关内容。即便由此获得资料（提供来源并经查实的例外）并作为向采购人或采购代理机构或监督管理部门提出异（质）疑或投诉或法院起诉的理由，均属于非法索取的依据。 3、质疑、投诉人未按前列序号第 17、18 条规定进行质疑、投诉（申诉）、举报等，均属于扰乱政府采购市场，直至公示。
20	解释：本采购文件的解释权属于招标采购单位。

一、总则

（一）适用范围

本采购文件仅适用于本次竞争性磋商采购所叙述的货物和服务。（法律、法规另有规定的，从其规定）。

（二）定义

1.“招标采购单位”系指德清天勤会计师事务所有限责任公司（采购代理机构）和德清县公安局（采购单位）。

2.“磋商响应方”系指向需方提交采购响应文件的供应商。

3.“服务”系指按竞争性磋商文件要求的服务。

4.“项目”系指磋商响应方按采购文件规定向采购人提供的产品和服务。

5.“书面形式”包括信函、传真、电报、电子邮件等。

6.带“▲”条款为实质性响应条款，必须响应。

（三）竞标委托

磋商响应方代表须携带身份证件。如磋商响应方代表不是法定代表人，须有法定代表人出具的授权委托书（正本用原件，副本可用复印件，格式见附件）。

（四）费用

不论磋商结果如何，磋商响应方均应自行承担所有与磋商有关的全部费用（采购文件有相反规定除外）。

（五）联合体

本项目不接受联合体。

（六）转包与分包

1.本项目不允许转包。

2.本项目不可以分包。

（七）特别说明：

1.磋商响应方所使用的资格、信誉、荣誉、业绩与企业认证必须为本企业所拥有。在组织商务、技术评审或资格性审查时，不得将属于供应商母公司或者同一母公司下属的其他子公司（以分支机构参与竞标的不得将属于供应商总机构或同一总机构下属的其他分支机构）的人员、业绩、荣誉、知识产权、项目案例等，作为该供应商的资信文件予以确认或审查通过。

2.磋商响应方应仔细阅读采购文件的所有内容，按照采购文件的要求提交采购响应文件，并对所提供的全部资料的真实性承担法律责任。

3.竞标人在竞标活动中提供任何虚假材料,其竞标无效，并报监管部门查处。中标后发现的,将没收中标人保证金，造成其他损失的须赔偿相应损失，且民事赔偿并不免除违法竞标人的行政与刑事责任。

4.根据浙江省财政厅《关于印发浙江省政府购买服务采购管理暂行办法的通知》（浙财采监〔2014〕28 号）规定，通过公开竞争的政府采购方式确定的原项目承接主体服务期满并通过验收，绩效评价好、服务对象满意度高的，在年度预算能够保障的前提下，可以根据原采购合同的约定续签合同，但续签的单次合同期限一般不得长于原采购的合同期限，且续签次数最多不超过 2 次、累计时间最长不超过 5 年。

5.根据《政府采购竞争性磋商采购方式管理暂行办法有关问题的补充通知》（财库〔2015〕124 号）的规定，提交最终报价的供应商可以为 2 家。

6.根据中华人民共和国财政部令第 87 号--《政府采购货物和服务招标投标管理办法》的规定，采用最低评标价法的采购项目，提供相同品牌产品的不同投标人参加同一合同项下投标的，以其中通过资格审查、符合性审查且报价最低的参加评标；报价相同的，由采购人或者采购人委托评标委员会按照招标文件规定的方式确定一个参加评标的投标人，招标文件未规定的采取随机抽取方式确定，其他投标无效。

使用综合评分法的采购项目，提供相同品牌产品且通过资格审查、符合性审查的不同投标人参加同一合同项下投标的，按一家投标人计算，评审后得分最高的同品牌投标人获得中标人推荐资格；评审得分相同的，由采购人或者采购人委托评标委员会按照招标文件规定的方式确定一个投标人获得中标人推荐资格，招标文件未规定的采取随机抽取方式确定，其他同品牌投标人不作为中标候选人。

非单一产品采购项目，采购人应当根据采购项目技术构成、产品价格比重等合理确定核心产品，并在招标文件中载明。多家投标人提供的核心产品品牌相同的，按前两款规定处理。

7. 小微企业价格扣除的有关政策：根据财库〔2011〕181 号的相关规定，在评审时对小型和微型企业提供小型、微型企业产品的报价给予 6 %的扣除，取扣除后的价格参与评审（仅对符合小微企业价格扣除政策的产品进行价格扣除，供应商需在报价明细表中单独列明符合小微企业价格扣除政策的产品及价格，扣除后的价格仅作为价格分计算）。供应商需在采购响应初次报价文件中同时提供《中小企业声明函》、磋商响应企业及所提供产

品制造企业在“国家企业信用信息公示系统——小微企业名录”的页面查询结果（加盖单位公章）。(注：未按以上要求提供材料的，均不给予价格扣除，符合价格扣除政策的成交人产品将在评审报告中予以公示。)

根据〔2017〕141 号的相关规定，在政府采购活动中，残疾人福利性单位视同小型、微型企业，享受评审中价格扣除政策。属于享受政府采购支持政策的残疾人福利性单位，应满足财库〔2017〕141 号文件第一条的规定，并在磋商响应初次报价文件中提供残疾人福利性单位声明函（见附件）。

（八）质疑和投诉

1.质疑、投诉应当采用书面形式，质疑书、投诉书均应明确阐述采购文件、招标过程或成交结果中使自己合法权益受到损害的实质性内容，提供相关事实、依据和证据及其来源或线索，便于有关单位调查、答复和处理。

2.供应商未按规定要求提出的，则视同认可采购文件，但法律法规及规范性文件有明确规定的除外。

二、采购文件

（一）采购文件的构成。本采购文件由以下部份组成：

1.竞争性磋商公告
2.竞争性磋商须知
3.采购内容及技术要求
4.磋商原则和程序
5.合同主要条款
6.磋商响应文件格式
7.本项目采购文件的澄清、答复、修改、补充的内容

（二）磋商响应方的风险

磋商响应方没有按照采购文件要求提供全部资料，或者磋商响应方没有对采购文件在各方面作出实质性响应是磋商响应方的风险，并可能导致其竞标被拒绝。

（三）采购文件的澄清与修改

1.在磋商截止时间前，采购代理机构对已发出的采购文件进行必要澄清或者修改时，将依法在财政部门指定的政府采购信息发布媒体上发布更正公告，并以书面形式通知所有采购文件收受人，除书面答复以外的其他澄清方式及澄清内容均无效。该澄清或者修改的内容为采购文件的组成部分，对所有磋商响应方有约束力。磋商响应方在收到采购文件的澄清修改函后，应以书面形式予以确认。

2. 采购代理机构可以视采购具体情况，延长磋商截止时间和磋商时间，并依法在采购文件要求提交磋商响应文件的截至时间 2 日前，将变更时间书面通知所有采购文件收受人，并在财政部门指定的政府采购信息发布媒体上发布变更公告。

3.采购文件澄清、答复、修改、补充的内容为采购文件的组成部分。当采购文件与采购文件的答复、澄清、修改、补充通知就同一内容的表述不一致时，以最后发出的书面文件为准。

4.采购文件的澄清、答复、修改或补充都应该通过本代理机构以法定形式发布，采购人非通过本机构，不得擅自澄清、答复、修改或补充采购文件。

三、磋商响应文件的编制

注：磋商响应方应保证所提供文件资料的真实性，所有文件资料必须是针对本次竞标

的。如发现磋商响应方提供了虚假文件资料，其竞标将被拒绝，并自行承担相应的法律责任。

（一）磋商响应文件的组成

磋商响应文件由资信及商务文件、技术文件和初次报价文件三部份组成。凡是参加两个或者以上标项竞标的，磋商响应文件必须按标项分别制作、分别密封，各标项磋商响应文件一正本二副本，且必须按标项分别单独包装、单独提交。如磋商响应方不按上述规定制作磋商响应文件的，可能导致被拒绝。

1. 资信及商务文件（一正本二副本，封装成一袋。）：

（根据《浙江省财政厅关于印发浙江省政府采购供应商注册及诚信管理暂行办法的通知》（浙财采监字[2009]28 号），凡浙江省政府采购注册供应商，且本项目规定所需的资格审查文件已在注册供应商库中上传的。则在制作竞标文件时，可凭网上打印且每一页都经法定代表人签字和加盖公章后的“浙江省政府采购注册供应商信息登记表”等证明材料，代替相应的竞标资格证明原件，在竞标文件中免于提供相关的书面资格材料原件，但应当对其网上注册信息的真实性和有效性等承担责任。）

A. 资格审查部分（竞标时可另外准备一份胶装成册并单独密封的资格审查文件在响应截止时间前单独提交）：

a.磋商响应方的有效工商营业执照或法人证书复印件加盖公章；（原件备查）

b.磋商响应供应商的依法缴纳税收（投标截止时间前近三个月缴纳增值税和企业所得税的完税凭据或税务部门出具的其他证明）和社会保障资金（投标截止时间前近三个月缴纳社会保险的凭证（专用收据或社会保险缴纳清单）或人社部门出具的其他证明）证明材料复印件加盖公章；（原件备查,依法免税或不需要缴纳社会保障资金的供应商，应提供相应文件证明其依法免税或不需要缴纳社会保障资金。）

c.供应商市场行为信誉（信用）情况承诺书原件（格式见附件，网站截图可由磋商响应方自行提供或磋商时由采购人或采购代理机构查询作为资格证明材料）；

d.法定代表人授权书原件、授权代表身份证（原件查看）复印件一份；（磋商时，请另行准备一份法定代表人授权委托书原件及携带有效身份证明原件）

e.磋商响应供应商的其他投标资格证明文件复印件加盖公章（若供应商为总公司所设立的区域性分支机构（分公司），以及个体工商户、个人独资企业、合伙企业需提供房产权证、车辆行驶证或其他固定资产等有效财产证明材料复印件加盖公章）。（原件备查）

B.声明书（格式见附件）；

C.磋商响应方基本情况一览表（格式见附件）；

D.磋商响应方的最近一个季度公积金的证明；

E.2018 年 9 月 30 日资产负债表及 2018 年 7-9 月份的利润表（复印件加盖公章）；

F.2017 年度财务审计报告；

G.磋商响应方的公司及公司的技术团队情况；

H.“信用中国”网站（www.creditchina.gov.cn）查询守信红名单记录（若有）；

I.磋商响应方的荣誉（相关证书）（具体可参考评分项，复印件加盖公章，原件备查）；

J.项目业绩表（格式见附件）附上合同复印件、相关证明材料（加盖公章，原件备查）；

K.商务响应表（格式见附件）（加盖公章）；

L.磋商响应方为中小企业，或按规定享受其他国家政策支持、扶持的相关证明材料（中小企业声明等）；

M.优惠条件或服务措施情况

N.采购文件要求的，以及磋商响应方认为要说明的其他内容。

2、技术文件：（一正本二副本，封装成一袋。）

A、对本次项目的理解和技术方案总体设计及实施；

B、根据第三章采购内容与技术要求中的相关要求，与其一一对应并且响应情况；须提供相关证明材料、检测报告、原厂商质保等承诺的，格式自拟；

C、官网加固方案；

D、考察并了解大会官网相关情况，提供相关材料；

E、根据大会官网现状提出有关网站加固的相关建设性意见；

F、备份节点机房的相关情况；

G、人员配备情况（格式自拟，相关证书、证明文件需提供复印件并提供人员社保，原件备查）；

H、应急响应方案；

I、技术和服务偏离说明表(格式见附件)；

J、针对本项目提出的合理化建议（若有）；

K、采购文件要求的以及磋商响应方认为可能需要说明的其他文件资料。

3、初次报价文件：（一正本二副本，封装成一袋。）

A. 采购响应函（格式见附件）；

B. 磋商初次报价一览表（格式见附件）；

C. 磋商初次报价明细表（格式自拟）；

D. 磋商响应供应商《中小企业声明函》及磋商响应供应商在“国家企业信用信息公示系统——小微企业名录”的页面查询结果**（若符合价格扣除情形的提供此项）；**

E. 磋商响应供应商所投产品制造企业在“国家企业信用信息公示系统——小微企业名录”的页面查询结果**（若符合价格扣除情形的提供此项）。**

▲注：法定代表人授权委托书、投标声明书、投标函、供应商市场行为信誉（信用）情况承诺书由法定代表人签名（或盖法人章）并加盖单位公章。（法定代表人亲自参加开标的不需要提供法定代表人授权委托书）

（二）磋商响应文件的语言及计量

▲1 磋商响应文件以及竞标方与采购方就有关竞标事宜的所有来往函电，均应以中文汉语书写。除签名、盖章、专用名称等特殊情形外，以中文汉语以外的文字表述的磋商响应文件视同未提供。

▲2 竞标计量单位，采购文件已有明确规定的，使用采购文件规定的计量单位。采购文件没有规定的，应采用中华人民共和国法定计量单位（货币单位：人民币元），否则视同未响应。

（三）磋商报价

1.磋商报价应按采购文件中相关附表格式填写。

▲2.磋商报价是履行合同的最终价格，须包括须包括服务款、专用工具、保险、税金等，招标范围内全部工作内容等一切费用。磋商报价为磋商响应方所能承受的最低、最终一次性报价。供应商的报价为整个采购项目的总报价，报价明细表如有漏项，视同漏项内容已包含在其总报价中，合同总价不做调整。

▲3.磋商响应文件只允许有一个报价，有选择的或有条件的报价将不予接受。

▲4.本次项目的代理费由中标供应商承担，按中标金额的相应比例收取，100 万元以下按 1.5%，100-500 万按 0.8%。

▲5. 磋商响应方对同一竞标产品不得同时出现可选择性品牌和一个品牌中的可选择性型号。

6. 磋商响应文件中的单价、合价、总价全部采用人民币表示。

（四）磋商响应文件的有效期

▲1.自磋商截止日起 90 日历天磋商响应文件应保持有效。有效期不足的磋商响应文件将被拒绝。

2.在特殊情况下，采购人可与磋商响应方协商延长竞标书的有效期，这种要求和答复均以书面形式进行。

3.磋商响应方可拒绝接受延期要求而不会导致磋商保证金被没收。同意延长有效期的磋商响应方需要相应延长磋商保证金的有效期，但不能修改磋商响应文件。

4.成交人的磋商响应文件自磋商之日起至合同履行完毕止均应保持有效。

（五）磋商保证金

▲1.磋商响应方须按采购文件规定的时间和形式提交保证金。否则，其竞标将被拒绝。

2.保证金形式：汇票、电汇、支票等非现金形式

3.未中标的磋商响应方的保证金，在成交通知书签发后的 5 个工作日内退还。磋商响应方须按保证金代退程序要求，及时提供退还保证金所需的收款收据及帐户信息，若因上述原因而导致保证金未能及时退还的，责任由磋商响应方承担。

4.成交人签订合同后，由采购代理机构按保证金代退程序要求退还其磋商保证金。

5.▲磋商保证金一律采用信汇或电汇方式退还。

【建议磋商响应方提交响应文件的同时，单独密封提交本磋商响应方的银行帐户资料和退投标保证金的往来款收据（客户名称填德清天勤会计师事务所有限责任公司，往来项目填保证金，金额填本次项目交纳的保证金数额，并填明开票人和开票日期，加盖本磋商响应方的财务专用章及公章），便于退还投标保证金（磋商响应方不用再次到采购代理机构办理退还手续）。】

6.磋商响应方有下列情形之一的，磋商保证金将不予退还：

（1）磋商响应方在磋商文件有效期内无故撤销竞标文件的；

（2）未按规定提交履约保证金的（如有）；

（3）磋商响应方在磋商过程中弄虚作假，提供虚假材料的；

（4）除不可抗力外，供应商在定标后领取成交通知书前恶意弃标（或无故撤销竞标文件的）或拒绝在成交通知书规定期限内签订合同的，不仅保证金不予退还，还要赔偿合

同差价，同时不得再参加本项目重新组织的采购活动；

（5）将成交项目转让给他人或者在磋商响应文件中未说明且未经采购单位同意，将成交项目分包给他人的；

（6）拒绝履行合同义务的；

（7）其他严重扰乱竞标程序的；

（8）法律法规规定的其他情形。

（六）磋商响应文件的装订、签署和份数

1.磋商响应方应按本采购文件规定的格式和顺序编制、装订磋商响应文件并标注页码，磋商响应文件内容不完整、编排混乱导致磋商响应文件被误读、漏读或者查找不到相关内容的，是磋商响应方的责任。

2.磋商响应方应按资信及商务文件、技术文件和初次报价文件正本各 1 份，副本各 2 份分别编制并单独装订成册，磋商响应文件的封面应注明“正本”、“副本”字样。活页装订（纯订书钉、活页夹装订等使标书可以拆卸或者在翻动过程中易脱落的装订形式将被认定为活页装订）的磋商响应文件（包括报价文件）按无效标处理，须胶封装订。

凡是参加两个或者以上标项竞标的，磋商响应文件必须按标项分别制作，各标项磋商响应文件一正本二副本，且必须按标项分别单独密封、单独提交。如磋商响应方不按上述规定按标项分别单独密封、单独提交磋商响应文件的，将可能导致被拒绝。

3.磋商响应文件的正本需打印或用不褪色的墨水填写，磋商响应文件正本除本《磋商响应方须知》中规定的可提供复印件外均须提供原件。副本可以为正本的复印件。副本为原件时，可与正本具有同等法律效力。正本副本内容不一致时，以正本为准。

4.磋商响应文件须由磋商响应方在规定位置盖章并由法定代表人或法定代表人的授权委托人签署，磋商响应方应写全称。

5.磋商响应文件不得涂改，若有修改错漏处，须加盖单位公章或者法定代表人或授权委托人签字或盖章。磋商响应文件因字迹潦草或表达不清所引起的后果由磋商响应方负责。

（七）磋商响应文件的包装、递交、修改和撤回

1.磋商响应方应按资信及商务文件、技术文件和初次报价文件三部分分别密封封装磋商响应文件。磋商响应文件的包装封面上应注明磋商响应方名称、磋商响应方地址、磋商响应文件名称（资信/商务文件或者技术文件等）、竞标项目名称、项目编号、标项及“磋商时启封”字样，并加盖磋商响应方公章。

2.如果磋商响应文件密封袋未按规定密封或未加盖公章，采购代理机构有权予以拒绝此磋商响应文件，并退回磋商响应方。同时，由此造成磋商响应文件被误投或提前拆封的风险由磋商响应方承担。

3.磋商响应方在磋商截止时间之前，可以对已提交的磋商响应文件进行修改或撤回，并书面通知采购单位。磋商截止时间后，磋商响应方不得撤回、修改磋商响应文件。修改后重新递交的磋商响应文件应当按本采购文件的要求签署、盖章和密封。

4. 如果因磋商响应文件密封不严、标记不明而造成过早启封、失密等情况，采购代理机构概不负责。

5.在磋商截止时间之后递交的磋商响应文件将被拒绝。

6.未在响应截止时间前提交报名资料的采购响应文件将被拒绝。

（八）竞标无效的情形

1.在符合性审查和商务评审时，如发现下列情形之一的，磋商响应文件将被视为无效：

（1）未按采购文件规定交纳磋商保证金的；

（2）超出经营范围竞标且法律法规规定属于限制经营或需前置性经营许可的；

（3）磋商时不能按采购文件要求提供相应的资格证明文件进行资格审查的，或者不符合采购文件标明的资格要求的；

（4）磋商响应文件所有的声明书、投标函、供应商市场行为信誉（信用）情况承诺书和法定代表人授权书原件均无法定代表人签名(或盖法定代表人私章)、没有盖单位公章的,或未按采购文件规定格式提供投标声明书、投标函、供应商市场行为信誉（信用）情况承诺书和法定代表人授权书原件的；**（法定代表人亲自参加开标的不需要提供法定代表人授权委托书）**

（5）磋商响应文件内容不真实的；

（6）磋商响应文件的实质性内容含义不明确、同类问题表述不一致或者有明显文字和计算错误，或者使用计量单位不符合采购文件要求的（经磋商小组认定并允许其当场更正的笔误除外）；

（7）未实质性响应采购文件要求或者磋商响应文件有采购人不能接受的附加条件的；

（8）“资格信息登记表”及其网上注册登记的信息与本采购文件规定的资格条件不符，且未在采购响应文件中说明并未补充提供相关书面资格证明材料的；

（9）与采购文件中标“▲”的条款及采购文件其他要求发生实质性负偏离的；

（10）磋商响应方的法定代表人或其授权代理人未能准时参加磋商会议的；

（11）磋商时磋商响应方的法定代表人或其授权代理人未能当场出具有效身份证明，或供应商代表与法定代表人授权委托人身份不符的；

（12）竞标产品（或服务）载明的验收标准和方法等不符合国家规定的；

（13）不符合法律、法规和采购文件规定的其他实质性要求（磋商小组一致认定）的；

（14）磋商响应文件未装订、活页装订（纯订书钉、活页夹装订等情况将被认定为活页装订，建议采用胶封装订）的；

（15）本采购文件中其他规定磋商响应文件无效的情形。

2.在技术评审时，如发现下列情形之一的，磋商响应文件将被视为无效：

（1）未提供或未如实提供竞标产品的技术参数，或者磋商响应文件标明的响应或偏离与事实不符或虚假竞标的；

（2）明显不符合采购文件要求的规格型号、质量标准，或者与采购文件中标“▲”的参数指标要求发生实质性负偏离的（磋商小组一致认定）；

（3）竞标产品的技术规范、技术标准明显不符合国家强制性要求的；

（4）竞标技术方案不明确，存在一个或一个以上备选（替代）磋商响应方案的；

(5)与其他参加本次磋商响应方的磋商响应文件（技术文件）的文字表述内容相同连续20行以上或者差错相同2处以上的。

3.在报价评审时，如发现下列情形之一的，磋商响应文件将被视为无效：

（1）未采用人民币报价或者未按照采购文件标明的币种报价的；

（2）磋商报价具有选择性；

（3）磋商小组认为竞标人的报价明显低于其他通过符合性审查竞标人的报价，有可能影响产品质量或者不能诚信履约的，要求其在评标现场合理的时间内提供书面说明，并提交相关证明材料，但竞标人不能证明其报价合理性的；

（4）二分之一以上的评委认为供应商报价明显高于市场平均价的；

（5）磋商报价超出采购预算的（或采购文件规定的价格上限）。

(6)法律法规和采购文件规定的其他无效情形。

4.被拒绝的磋商响应文件为无效。

第三章 采购内容及技术要求

一、 说明

1. 本采购文件所提出的货物技术标准是基本的技术标准和使用功能，并未规定所有的技术要求和适用标准，供应商应提供一套满足所列标准要求的高质量的产品及相应服务。本技术要求使用的标准如与供应商所执行标准发生矛盾时，按较高标准执行。

2. 本采购货物应按国际标准、国标、部标或专业标准制造；非标准货物按采购人提供的要求制造；质量标准按照国家有关规定及合同约定进行验收。

3. **带▲号的条款内容，为本次采购的主要条款和实质性内容，磋商响应方必须完全响应。**

二、 相关要求：

1.1. 建设背景

首届联合国世界地理信息大会将于 2018 年 11 月在浙江德清举行。大会由联合国主办，国家测绘地理信息局和浙江省人民政府共同承办。此次大会不仅是联合国主办的规模最大、级别最高、内容最丰富的地理信息大会，也是测绘地理信息领域迄今为止在中国举办的层次最高、覆盖面最广的重大国际多边活动。大会将交流展示世界测绘地理信息领域的最新进展，展望未来发展趋势，研讨地理信息支撑联合国 2030 年可持续发展议程实施的举措，提出共同应对各国及全球面临挑战的倡议。

为确保地信大会成功举行，全面提升主站的整体安全防护水平，须针对大会官网系统建立安全加固保障服务。并提供统一的云防护接入、安全监测扫描、备份机房节点、应急响应、安全配置核查、应急预案编制及应急演练等服务，保证在事前第一时间掌握、了解、网站系统可访问性、安全状态，及时发现、预警网站安全问题，确保大会顺利召开。

1.2. 招标内容

序号	服务项	内容描述	数量和服务期限
1	云防护服务	针对大会官网系统提供云安全防护服务，实现对 Web 应用系统实时防御，包括：各类注入攻击、跨站攻击、Webshell、扫攻击、敏感信息泄露、盗链、DDoS 等；提供一键关停、永久在线服务，服务期间提供安全防御日报和重大安全事件告警，包括应用系统访问流量、访问详情、攻击详情、应用系统潜在问题分析等；定期提供云安全防护月报、季报、年报；提供 7x24 小时安全专家运维服务，为用户提供专业的网站安全运维，协助用户处理安全问题。	提供 1 个主域名，以及不低于 20 个子域名的云防护服务，服务期限 2 年
2	Web 安全监测服务	针对大会官网提供 7x24 小时监测服务，具体包括网站漏洞监测、篡改监测、网马及暗链监测、网站可用性、网站敏感信息实时监测。根据 7x24 小时监测结果，及时预警、取证并输出报告；并及时提供监测报告。同时提供专业的网站安全漏洞检查工具，实现对大会官网开展远程安全扫描和漏洞检查，汇总扫描及检查结果，在大会重保期间以日报形式提供相关安全漏洞扫描报告。	提供 1 个主域名，以及不低于 20 个子域名的 Web 安全监测服务，服务期限 2 年
3	官网备份节点机房	在物理数据中心机房环境部署大会官网的备份节点，涉及备份节点的安全防护措施应参考主平台的安全配置。一旦主站出现紧急情况时，	大会重保期内提供官网 1 个备份节点

		可第一时间切换至备用节点，保障大会官方网站访问畅通。	资源
4	官网备份节点机房安全管理平台	通过汇聚各类安全能力，提供包含漏洞发现、安全防御、审计追溯等覆盖全生命周期的安全产品服务，为异地物理机房备份节点构建一个统一管理、弹性扩容、按需分配、安全能力完善的安全资源池。安全平台应至少包含堡垒机、防火墙、数据库审计、日志审计、网页防篡改、主机安全等服务模块。	大会重保期内提供官网 1 个备份节点的安全防护
5	网络架构分析服务	为大会官网提供基于需要分析的整体网络或者目标区域网络的架构分析，对整体网络中的脆弱点进行有效识别。	大会重保期间提供 1 次网络架构分析服务
6	应急响应服务	应急响应服务内容包括且不限于对意外事故的处理、非法入侵的处理和调查恢复、网络攻击的应急防护等。 提供 7x24 小时的应急支持，当出现针对官网系统的安全风险、恶意攻击、入侵等威胁时，在 2 小时之内到达现场并提供安全应急响应服务（重保时期驻场人员 5 分钟内响应），协助查找风险来源，确定威胁过程，提供故障恢复方案，并协助进行修复加固。	大会重保期间提供应急响应服务
7	安全漏洞评估服务	使用网络安全远程漏洞评估工具，检测网络设备、操作系统、数据库和应用服务中存在的安全漏洞，提供漏洞评估报告和修复建议。	大会重保期间提供 2 次安全漏洞评估服务，资产数量不超过 50 个
8	安全配置评估服务	使用网络安全配置核查工具或人工方式，对系统中网络设备、操作系统、数据库和应用服务器的配置进行安全检查，提供安全配置评估报告和改进建议。	大会重保期间提供 2 次安全配置评估服务，资产数量不超过 50 个
9	协助安全加固服务	针对安全漏洞和安全配置评估中发现的安全漏洞和配置缺陷，提供加固意见和方案，配合招标人完成配置修复。	大会重保期间提供 2 次协助安全加固服务，资产数量不超过 50 个
10	源代码安全审计服务	采用业界认可的专业代码审计工具，依据 OWASPTOP10 漏洞，通过工具扫描、人工确认、人工代码抽查等方式，对 Web 应用进行脆弱性安全检查，发现源代码中存在的安全风险。	大会重保期间提供两次不低于 55 万行的源代码安全审计服务
11	应急预案编制服务	根据重大时期安全保障要求，制定专项应急预案，包含网络攻击、数据篡改、数据泄漏等攻击行为应急处置流程，明确汇报方式，保障应急有效性。	大会重保期间提供 1 次应急预案编制服务
12	安全配置策略定制服务	结合招标人实际安全需求，协助定制安全配置规范（包括操作系统、数据库、中间件、网络设备、安全设备等），用于编写配置核查系统规则，实现快速自动化安全配置检查工作。	大会重保期间提供 2 次安全配置策略定制服务，资产数量不超过 50 个
13	恶意样本分析服务	人工方式检测操作系统和应用中是否存在恶意样本，分析样本的访问行为，评估对系统的影响，提供安全分析报告和清除方法。	大会重保期间提供 2 次恶意样本分析服务
14	安全演练设计服务	根据重大时期安全保障要求，提供专项预案，准备演练场景，以模拟演练的方式检验应急预案和应急流程是否完善，提高应急处理能力。	大会重保期间提供 2 次安全演练设计服务
15	安全渗透测试服务	通过人工黑盒的测试方式，采用独特测试手法，发现网络和业务系统中网络和系统存在的安全缺陷，提供渗透测试报告和改进建议，主要包括逻辑缺陷、上传绕过、输入输出校验绕过、数据篡改、功能绕过、异常错误以及其他专项内容。	大会重保期间提供 2 次安全渗透测试服务，域名数不超过 20 个
16	主动诱捕服务	通过在用户在内网部署多个专业诱捕攻击节点（陷阱），当攻击者攻入系统时，触碰到诱捕节点，立即告警。	大会重保期间提供 1 项主动诱捕服务

17	可信众测服务	采用可信众测模式，选取安全专家模拟真实黑客对网站进行真实的渗透测试，协助采购人发现潜在安全风险。	大会重保期间提供1次可信众测服务
18	移动APP安全测试服务	对移动APP程序进行安全测试，发现可能存在的安全缺陷，提供安全测试报告和改进建议。	大会重保期间提供2个APP安全测试服务
19	定制安全通告服务	实时关注安全动态，在安全保障期间，为采购人提供安全通告服务。该通告包括安全漏洞(补丁)通告、安全威胁通告、安全业界动态、恶意代码防范、紧急通告等多项内容。	大会重保期间提供2次定制安全通告服务
20	安全值守保障服务	保障期间，安排具有大型网络系统安全保障经验、攻防经验的专家以现场方式提供安全保障工作，协助处理信息安全事件。	大会重保期间提供安全值守保障服务
21	日志安全分析服务	通过专业日志分析系统对各类系统（IDS、WEB服务器等）产生的日志进行数据分析，及时发现攻击事件和可疑行为，提供日志分析报告。	在大会重保期间提供每日1次的日志安全分析服务
22	安全运营服务	保障期间针对系统开展全面资产核查、配置管理、安全日志审计、攻击行为审计、攻击阻断等全面安全运营管理服务，并根据相关安全状态生成相关记录及汇报材料。	在大会重保期间提供3人驻守的安全运营支撑服务
23	云资源	为大会官网提供国内主流公有云平台资源，平台自身须通过等级保护三级测评。	云服务器10台、云数据库3台、30M带宽。 服务期限详见清单
24	云防篡改软件	为大会官网提供网站防篡改、防攻击服务，作为网站的最后一道安全防线。	大会重保期间提供1套防篡改软件
25	云堡垒机	为大会官网提供虚拟机、数据库等远程运维权限管理，实现运维人员双因素认证，且对整个运维过程进行录像。	大会重保期间提供授权资产50个
26	云主机安全	为大会官网提供服务器安全运维管理，通过安装在服务器上的轻量级Agent插件与云端防护中心的规则联动，实时感知和防御入侵事件，保障服务器的安全。	大会重保期间提供8台云主机的安全模块
27	云日志审计	为大会官网提供综合日志分析能力，可收集服务器、网络设备、安全设备的日志进行分析。	大会重保期间提供授权20个资产的日志审计服务
28	云数据库审计	为大会官网提供云数据库审计服务，将数据库监控、审计技术与公共云环境相结合，支持对云平台中的数据库进行审计，针对数据库SQL注入、风险操作等数据库风险行为进行记录与告警，形成对核心数据的安全防护，提供完善的安全诊断、维护、管理功能。	大会重保期间提供3台云数据库审计服务

注：大会重保期间为：合同签订之日起至2018年12月31日

1.3. 技术参数

1.3.1云防护服务参数

服务项	技术要求
★产品节点规模	支持全国至少20个云防护节点以上，以支撑各个区域网站的安全防护能力。
★基本需求	无需在被防护网站上安装任何软件，采用B/S设计架构支持通过浏览器远程对网站进行配置、操作。
★Web攻击防护	支持服务器隐身，使得黑客无法获取服务器真实IP地址，防止黑客

	对服务器的各种攻击。
	交付时提供 HTTPS 网站防护。
	支持 HTTP/HTTPS 协议合规性检查，包括畸形报文、HTTP 版本检查、报文头缺失、请求方法限制、协议违规等。
	支持服务器敏感信息泄露防护，包括服务器类型信息、服务器版本信息、敏感路径信息泄露、网站源码泄露、数据库敏感信息泄露等。
	应能识别和阻断 SQL 注入攻击、Cookie 注入攻击、命令注入、跨站脚本攻击、文件包含攻击、LDAP 注入、XPATH 注入、爬虫攻击、Struts2 命令执行攻击等常见的 Web 攻击，防止网站敏感信息泄露或网站内容被恶意篡改。
	支持 ASP 木马、JSP 木马、PHP 木马、一句话木马等多种形式的 Web Shell 后门的上传防护。
	支持对 Appscan、Awvs、Pangolin、Burpsuite、啊 D、明小子、Nikto、等扫描器的扫描防护。
	支持 HTTP 参数污染、00 截断、url 编码绕过、Unicode 编码绕过、ASCII 码绕过、字符串拼接绕过、hex 编码绕过、大小写混杂字符绕过、多空格绕过、注释串绕过等多种绕过攻击防护。
	支持 Web 容器漏洞、数据库漏洞、CMS 插件漏洞等漏洞攻击防护。
	支持自定义防护页面功能，即当检测到 4、5 开头的响应码时可以跳转到指定 URL 以提高服务感受和搜索引擎 SEO。
★DDOS 攻击防护	支持对 Sys Flood 攻击、Tcp Flood 攻击、Ack Flood 攻击、Udp Flood 攻击、Icmp Flood 攻击、Rst Flood 攻击、慢速攻击等常见的 DDOS 攻击进行流量清洗。
	支持对 TCP/UDP/IP 等类型的畸形报文攻击进行防护、支持对 Smurf 攻击、Land 攻击、Fraggle 攻击、Ping of Death 攻击等 DDOS 攻击进行流量清洗。 本次标项提供≥300G 防护能力 本次标项提供≥20 个域名防护
★CC 攻击防护	支持根据出入云平台流量来对攻击进行 CC 攻击判断，即攻击流量超出管理员配置流量阈值后，对攻击源进行 JS 防御或图片验证防御。
	支持根据源站总并发连接数和访问源单 IP 并发连接数对攻击进行 CC 判断，并发连接数超出管理员配置并发连接数阈值后，对攻击源进行 JS 防御或图片验证防御。
	支持根据服务器响应时间对访问源进行 CC 攻击判断，响应时间超出管理员配置响应时间阈值后，对攻击源进行 JS 防御或图片验证防御。
缓存加速	有全国性的缓存节点机房，按照最小响应时间，最优访问服务等智能缓存算法算法为用户自动选择缓存节点机房，以提升用户访问效果。
	支持 URL 缓存黑白名单功能，可以对特定 URL 进行是否缓存进行控制。
	支持浏览器缓存加速功能，即将待访问的内容缓存在访问者浏览器上，用户无需请求服务器即可完成对网站页面文件的访问。
	支持数据压缩，即对传输的页面文件进行数据压缩以提高传输效率。
	需要提供网站永久在线功能，即网站由于各种原因不能访问时，Web 应用防火墙可以提供网站首页映像，访问者可以访问到这个首页
一键关停	支持一键关停功能，当网站出现紧急安全事件时，可在一分钟内通过手机APP 和浏览器一键完成关停，防止产生严重后果。
日志报表	支持网站访问次数统计，访问 IP 数统计，PV 数统计，漏洞攻击数统计、CC 攻击数统计等攻击访问统计。
	每个二级域名有独有的攻击访问统计报表。

	支持 web 攻击统计报表，CC 攻击统计报表，CC 攻击 URL TopN 报表等。
	支持 Web 攻击报表，包括 web 攻击次数，攻击 IP 数，攻击者全国分布图，攻击 IP TopN。
	Web 攻击日志至少包含攻击类型、攻击 IP、IP 归属地、攻击 URL 及参数，攻击次数等参数。
	CC 攻击报表包括 CC 攻击次数，攻击 IP 数，攻击者全国分布图显示，攻击 IP TopN，
	CC 攻击日志至少包含攻击类型、攻击 IP、IP 归属地、攻击 URL、攻击事件、攻击次数等参数。
	支持流量对比报表，能直观的展示回源流量与加速流量的对比及回源次数和加速次数的对比。
安全报表	支持安全周报功能，能直观的显示本周及历史周网站遭受的 Web 攻击、CC 攻击等攻击情况。
	周报内容包括本周拦截漏洞数、本周遭受的 CC 攻击数、本周攻击次数最多的 IP、本周受攻击最多的域名，本周 Web 攻击的趋势报表、本周遭受的 CC 攻击的趋势报表，本周 web 攻击方式 TopN、本周遭受 CC 攻击的 URL TopN，Web 攻击源 IP 全国分布位置，CC 攻击源全国分布位置等内容。安全报表支持 PDF 格式导出下载，安全周报支持 PDF 格式导出下载。

1.3.2 WEB安全监测服务参数

服务项		**技术要求**
监测内容要求	脆弱性监测	对网站存在的脆弱性进行探查，包括 SQL 注入漏洞、跨站脚本漏洞、开放服务漏洞、网站第三方应用漏洞等，及时发现漏洞
	安全事件监测	1、 对网站后门进行监测； 2、 对网站被植入暗链进行监测； 3、 对网站黑页进行监测； 4、 对网站首页、重要页面或者其他指定页面篡改变更进行监测； 5、 对网页敏感内容进行监测，如“博彩”、“色情”等；
	坏链监测	检测网站是否有错误链接
	挂马监测	1、 对网站进行挂马检测，能够检测出常见木马 2、 监测是否植入 shellcode 或可疑的外部链接
	DNS 域名解析监测	1、监测网站域名对应的 IP 地址是否变化 2、监测 DNS 是否被劫持或过期
	可用性监测	1、监测网站服务是否中断或报错 2、监测网站延时是否过大 3、通过多线路监测是否存在线路异常
监测报告要求	安全监测月报	网站总体安全状况、本月与前几月的差异分析统计、网站漏洞情况统计及详细描述、网页木马情况统计及详细描述、网页篡改情况统计及详细描述、网页关键字情况统计及详细描述、网站可用性情况统计及详细描述。
	年度安全分析报告	年度网站信息安全运行状况分析，重大安全事件或隐患分析，网站信息安全指数排名、重大安全事件处理情况。

告警要求	可用性告警	网站服务中断持续超过约定时长，提供电话、密信、邮件告警
	安全事件告警	监测到网页被篡改、被植入暗链、webshell、网页木马等，提供电话、邮件告警
	安全通报 APP 功能	具有国家密码管理局颁发的商用密码产品销售证的安全告警手机应用 APP，能够通过平台发送告警至用户的 APP。

1.3.3 官网备份节点机房参数

服务项	技术要求
★资质要求	具备工信部颁发的增值电信业务经营许可证（因特网数据中心业务），需提供证书复印件，原件备查
双路市电	数据中心须配备双路市电，且入局方向实现冗余（需提供双路电接入证明文件）
柴油发电机	数据中心须配备柴油发电机组，油箱储油量须满足 4 小时后备时间，柴油发电机须实现自启
机柜双电源	数据中心机柜侧须实现双路 UPS 供电，以实现冗余
视频监控	数据中心须配备视频监控、门禁系统，并提供 7x24 小时安保值守
动环监控	数据中心须配备动力环境监控系统，并提供 7x24 小时动力应急值守

1.3.4 官网备份节点机房安全管理平台参数

模块	指标项	技术要求
安全平台参数		
云安全管理平台	★部署方式	云安全资源池实现计算资源、存储资源、网络资源、网络功能资源、安全功能等 IT 基础资源的虚拟化
		支持所有安全产品部署在虚拟机资源上，安全产品根据规格按需获取安全资源池的 CPU、内存、存储、网络等资源并实现自动化部署
		资源池支持弹性扩容，包含安全资源池计算节点、安全产品种类、安全产品有效时间等
		资源池采用分布式存储，提供安全产品的高可用和物理节点的动态迁移
	★兼容性	能够适用于主流的云平台，如 Vmware、华为云、华三云、阿里云、品高云、基于开源 openstack 开发的云平台等
		提供开放的 API 接口，支持第三方品牌的安全产品接入平台管理，为用户提供灵活的安全产品组合方案。
	★云安全能力	能够利用下层物理/虚拟安全资源为用户提供一站式安全解决方案，包括虚拟防火墙、虚拟 IPS、虚拟化 web 应用防火墙、云堡垒机、虚拟化漏洞扫描（含网站漏洞扫描、系统漏洞扫描、数据库漏洞扫描、基线扫描）、云数据库审计、云日志审计、云主机防御（东西向流量

		隔离、防病毒）等。
		支持等级保护二级推荐套餐和等级保护三级推荐套餐，且支持用户根据业务规模自定义选择套餐规格，实现一键开通等级保护服务套餐（提供界面截图）
	用户认证	支持管理员权限和用户权限分离，管理员管理安全资源池的运营状态，用户管理自己的安全产品和安全数据，用户和用户之间安全数据隔离
		支持三权分立安全原则，可实现虚拟防火墙、虚拟 IPS、虚拟化 web 应用防火墙、网页防篡改、云堡垒机、虚拟化漏洞扫描、云数据库审计、云日志审计、云主机防御（东西向流量隔离、防病毒）等所有安全产品的角色统一授权，授权粒度精细到每一个安全产品的每一个角色，同时可以给用户批量授权，如一次性给用户 A 授权堡垒机的运维管理员角色，给用户 B 授权堡垒机的审计管理员角色
		支持用户认证统一，被授权的用户可以通过登录到云安全管理平台单点登录到各个安全产品，包括虚拟防火墙、虚拟 IPS、虚拟化 web 应用防火墙、网页防篡改、云堡垒机、虚拟化漏洞扫描、云数据库审计、云日志审计、云主机防御（东西向流量隔离、防病毒）等所有安全产品。
	策略管理	支持通过云安全管理平台直接给扫描下发扫描策略，并通过可视化图表展示扫描资产统计，漏洞数量 TOP5 资产，出现频率最高 TOP5 漏洞等信息
		支持在管理平台展示所有扫描出来的漏洞，并直接给扫描漏洞做忽略、误报等处理
	资产管理	支持通过管理平台统一添加资产自动同步到相关安全产品，添加主机资产自动同步到堡垒机、主机扫描，添加网站资产自动同步到网站扫务等，无需到不同的安全产品模块逐一添加
		支持按照业务给用户资产分组，支持创建业务的时候关联对应资产
		支持批量导入资产，并自动同步资产到下发到对应安全产品
	监控中心	支持管理员通过监控中心获取整个安全资源池的监控数据，支持用户通过监控中心获取自己的安全运维数据
		支持管理员查看每个安全虚拟机的资源占用信息，包含资源 ID / 别名，CPU 使用率、内存使用率、磁盘使用率，网络流入流出速率，并用可视化图表的方式展示 CPU、内存、磁盘占用趋势，网络总流入流出速率趋势
	许可管理	支持许可自动化导入激活安全产品，云安全管理平台会根据开通安全产品的规格、数量、时间周期等信息自动导入许可到安全产品，实现安全产品自动化激活，包括虚拟防火墙、虚拟 IPS、虚拟化 web 应用防火墙、网页防篡改、云堡垒机、虚拟化漏洞扫描、云数据库审计、云日志审计、云主机防御（东西向流量隔离、防病毒）等所有安全产品许可的自动化导入激活。
		支持许可按需消耗，资源池只记录许可总数，即消耗一个安全许可可以激活一个云堡垒机、或者一个云数据库审计、或者一个云综合漏洞扫描、或者一个云 WAF、或者一个网页防篡改、或者一个云综合日志审计、或者一个 EDR，支持两个许可合并激活一个高规格的安全产品
		支持许可包导入，通过扩展许可数量，扩展资源池允许激活的安全产品数量
平台安全产品模块参数		
综合漏洞扫描子模块	规格要求	支持网站、系统、数据库、基线扫描许可，每个模块支持 20 个以上 IP 地址

	主机扫描	支持 Windows 系列操作系统，支持 Linux 主流操作系统（Centos、Redhat、Debian、Fedora、Ubuntu、Suse 等），支持 Unix 主流操作系统（AIX、HPUX、Solaris 等）；
		具备弱口令扫描功能，提供多种弱口令扫描协议，包括 SMB、RDP、SSH、TELNET、FTP、SMTP、IMAP、POP3、MySQL、MSSQL、REDIS、RTSP 等协议进行弱口令扫描，允许用户自定义用户、密码字典。
		可根据端口识别出的软件版本提供可能存在的相关漏洞列表（非验证性漏洞列表）
	配置核查	产品提供系统安全配置核查功能，能够对主流操作系统、中间件的安全配置项目进行检查。
	★WEB 扫描	产品提供 Web 应用漏洞扫描功能，支持对 Discuz、大汉 CMS、PHPCMS、DEDECMS、ECSHOP、WordPress、eWebEditor、FCKeditor、Struts2 等国内外常见第三方组件扫描
		支持识别国内外主流 Web 应用防火墙品牌；
		支持识别被扫描目标对象的网站响应状态，能根据不同的响应状态直观呈现不同颜色标识；
		产品厂家应为《信息安全技术 Web 应用安全扫描产品安全技术要求》标准起草单位之一；提供相关证明材料。
		支持展示被扫描网站的结构树，并支持网站结构树的导出。
	数据库扫描	支持 Oracle、Mysql、SQLServer、DB2、informix、达梦、人大金仓的授权数据库漏洞扫描
云 WEB 应用防火墙子模块	规格说明	保护站点不少于 16 个、防护流量 100Mbps、HTTP 最大并发数 180000、HTTP 最大新建数 10000
	防御功能	能够识别恶意请求含：跨站脚本(XSS)、注入式攻击（包括 SQL 注入、命令注入 、Cookie 注入等）、跨站请求伪造等应用攻击行为
		识别 HTTP 报文常见的编码和编码攻击：URL 编码、Base64 编码、HTML 编码、16 进制编码等
		内置主流 Webshell 特征库，对上传内容进行检查，防止恶意 Weshell 上传
		能自动识别扫描器的扫描行为，并智能阻断多种扫描器的扫描行为
	WEB 访问行为合规	支持对访问流程的校验 可配置页面合规页面流程 可配置页面思考时间 违反合规的访问直接被拦截并产生告警日志 需提供第三方测评机构的检测报告
	CC 防护功能	支持多种算法检测方法：对指定 URL 访问速率、对指定 URL 访问集中度检测 支持多种条件匹配算法：可基于 URL、请求头字段、目标 IP、请求方法等多种组合条件进行检测支持挑战模式，招标人端访问时 WAF 发起 302 重定向与 js 挑战验证是真实招标人还是 CC 工具发起的访问 支持学习业务流量模型，在业务流量异常时开启 CC 防护，并支持启动配置阈值 支持基于地理位置的识别，可设置不同地理区域的检测算法 支持 CC 慢攻击

	地图态势分析与阻断	按地理区域对攻击次数等进行统计，通过地图展示，并在地图上可以指定某一地理区域进行访问控制，阻断此区域 IP 的访问
主机安全及管理系统子模块	规格要求	支持不少于 20 台云主机防护，包含病毒查杀、网站后门查杀、漏洞管理、性能监控、主机防火墙、WEB 应用防护、登录防护、防端口扫描等
	监控扫描	病毒查杀：内置业界领先的病毒查杀引擎，依托安全管理中心和大数据分析，实现对已知和未知恶意文件的检测和响应
		后门查杀：静态语法分析和动态行为分析相结合的检测手段，网站目录下所有文件进行深入检测，可对加密木马进行检测
		漏洞管理：一键检测和修复系统漏洞，保证系统不会被勒索病毒等恶意软件利用
	安全防护	微隔离：主机的东西向流量隔离，可对虚拟机之间的访问进行细粒度的权限控制。
		登录防护：规则支持五个任意维度(任意地理位置，任意 IP，任意域名，任意计算机名，任意时间)的系统登陆访问策略设置； 防暴力破解可发现勒索病毒的东西向传播行为；
		防端口扫描：自动锁定恶意的端口扫描行为并记录告警，防止端口被利用传播勒索病毒
云数据库审计子模块	规格要求	支持不少于 8 数据库实例，并发大于 16000TPS
	协议支持	支持 Oracle、SQL-Server、DB2、Informix、Sybase、MySQL 等六种主流数据库审计，支持 PostgreSQL、HANA、Teradata、Cache、人大金仓、达梦、南大通用等数据库审计，支持 MongoDB 数据库审计；
		支持对 SQLserver 2005 以上版本采用通讯加密的数据库，可以导入证书的方式实现审计解密；
	审计功能	支持数据库请求和返回的双向审计，支持返回字段和结果集、执行状态、返回行数、执行时长等内容，支持通过返回行数和内容大小控制返回结果集大小；
	智能发现	支持定期自动扫描数据库漏洞和不安全配置，提供漏洞扫描报告；
	安全审计	支持审计记录中敏感数据的模糊化处理，内置常见敏感数据掩码规则，支持自定义敏感数据掩码规则
	统计报表	系统提供内置多种报表模板库，内置的报表不少于 35 种
		支持根据单个数据库或逻辑数据库组生成报表
		报表支持严格按照塞班斯（SOX）法案、等级保护标准要求生成多维度综合报告；
	模型分析	支持对数据库自动建模及智能对异常行为告警功能；
		可通过行为轨迹图方式展示数据库访问行为；
		可基于账号、IP 地址、访问权限、招标人端工具等维度对行为模型做钻取分析、变更分析，对学习的安全基线以外的行为自动智能的进行告警；
		可以自动对比不同时期的行为模型，以区分其审计日志数趋势、用户、IP 地址、工具、访问权限的差异情况；
	故障排错	系统内置独立的故障排错系统，可以支持一键导出加密的系统调试日志，支持一键检测服务、许可证、流量等大部分常见常见故障的检测；
云综合日志审计子模块	工作模式	独立完成审计日志采集，不依赖于设备或系统自身的日志系统；
		采用解决方案包上传对产品进行功能扩展，无需要代码开发。
		支持不少于 20 个日志源
	性能规格	支持使用代理(Agent)方式提取日志并收集
	日志收集	支持目前主流的网络安全设备、交换设备、路由设备、操作系统、应用系统等

		设备厂家包括但不限于：Cisco(思科)，Juniper，联想网御/网御神州，F5，华为，H3C，微软，绿盟，飞塔(fortinet)，Foundry，天融信，启明星辰，天网，趋势，东软，Nokia，CheckPoint，Hillstone(山石)，安恒，珠海伟思，帕拉迪，apc，arbor，clam，戴尔（dell），Mcafee， Symantec（赛门铁克），citrix(思杰)，watchguard，中兴，阿帕奇，WINDOWS 系统日志，Linux/UNIX syslog、IIS、Apache 等；
		支持常见的虚拟机环境日志收集，包括 Xen、VMWare、Hyper-V 等
		支持基于内存的实时关联分析，跨设备的多事件关联分析
	日志分析	支持自定义条件都事件进行聚合
		进行关联分析的规则可定制
		支持根据资产价值、资产漏洞、针对漏洞的威胁事件三者进行威胁的自动关联分析（三维关联），所有的三维关联算法和准则以 CVE、Bugtraq、OWASP 公开协议和标准为为基础
	日志备份	极高的日志高查询性能，支持亿级的日志里根据做任意的关键字及其它的检索条件，在秒级里返回查询结果
	地理信息系统	内置 GeoSec 地理安全子系统，内置世界以及中国安全 GIS 地图，支持用地理地图展示来源威胁的趋势，支持用地理地图展示目的威胁的趋势，支持在地理地图上标注威胁事件的发生分布，内置 IP 地址到经纬度的转换库，支持以地理信息类进行统计的数据报表，支持切换 Google 地图（需要连通互联网）
云堡垒机子模块	规格要求	支持不少于 20 个资产、20 个字符并发连接
		支持常用的运维协议：SSH、TELNET、RDP、VNC、FTP、SFTP；可通过应用发布的方式进行协议扩展，如数据库 Oracle/MSSQL/MySQL/DB2 等运维招标人端工具、VMware vSphere Client/AS400 等远程管理工具
	基本功能	支持 oracle、mysql、sqlserver 数据库协议代理运维，可直接调用本地 windows 系统的数据库招标人端工具，支持自动登录、无需应用发布前置机。
		支持常用的运维协议：SSH、TELNET、RDP、VNC、FTP、SFTP；可通过应用发布的方式进行协议扩展，如数据库 Oracle/MSSQL/MySQL/DB2 等运维招标人端工具、VMware vSphere Client/AS400 等远程管理工具
		支持自动收集设备 IP、运维协议、端口号、账号、密码、与用户的权限关系，甚至可自动完成授权
		导出的设备信息文件加密存储，解密时须由 2 个管理员同时解密才能查看到设备信息文件内容
		支持定期自动修改 windows 服务器、网络设备、linux/unix 等目标设备密码功能。
	运维方式要求	在不依赖于应用发布的条件下，支持通过堡垒机页面直接调用本地 windows 的 plsql、sqlplus、sqlwb、ssms、mysql.exe 等数据库招标人端工具
		支持保存 SSH 的 sz/rz 命令（zmodem）传输的原始文件
		支持保存 SFTP/FTP 传输的原始文件
		支持保存 RDP 传输的原始文件
		支持自动化运维功能，可将结果通过邮件通知管理员；可对 linux/unix/windows 进行自动改密，可对 linux/unix/网络设备自动执行命令
		支持文件传输协议控制、命令控制、访问控制的三种安全策略
网页防篡改	基本要求	产品形态：软件形态，部署在网站服务器端

子模块		防篡改的 agent 支持的操作系统：Windows2000、2003、2008、2012、32&64 位、Redhat、CentOS、SUSE 等 32&64 位
		管理方式：B/S 管理方式、支持 windows、linux 平台
		采用先进内核驱动、WEB 核心内嵌和实时触发机制结合
		内核自定义编译：agent 支持云主机 Xen 内核
	防篡改功能	文件保护：支持各类网页文件的保护
		模板配置：支持在同一种操作系统下，网站路径相同，可通过规则模板，用模板统一将规则下发到各监控端，无需对监控端进行一一配置
		一键启停文件保护：一键启停所有监控端（agent）对文件开始 / 停止保护，不必登录 WEB 服务启进行停启
		Docker 容器：防护端 agent 兼容 docker 容器环境的部署
下一代防火墙子模块	工作模式	必须支持透明、路由、混合、旁路 4 种工作模式，同时支持旁路模式+在线模式部署
	规格要求	支持 FW/IPS/AV/VPN 等模块，吞吐量不少于 4G；
	攻击防护	支持 IPv4/6 抗应用型 DOS 攻击防护，如 HTTP Flood、DNS query flood 等攻击防护;支持抗流量型攻击防护，如 syn flood、udp flood、icmp flood，tcp flood 等攻击防护
		抗常见 DOS 攻击防护，jolt2、land_base、ping_of_death syn flag、tear_drop 、winnuke 、smurf、 ip spoof 等。
		支持 IP-MAC 绑定，支持对防火墙自身 DOS 防护和防止扫描功能
	VPN	支持 site to site 和远程接入 VPN 方式,支持主模式，野蛮模式，野蛮模式支持 FQDN、USER-FQDN 和通配符设置
		支持 VPN 零配置上线、VPN 批量下发
		支持专有 SSL VPN 招标人端，招标人端支持 Windows 32 位/64 系统，支持开源的 SSL VPN 招标人端系统包括 IOS 安卓 linux
	病毒防护	支持 HTTP，FTP，POP3，SMTP，IMAP 协议的病毒查杀、病毒库自动更新、虚拟脱壳、自定义查杀文件大小、查杀可疑病毒、可疑脚本、图片病毒、查杀邮件正文、附件、网页及下载文件中包含的病毒
		预定义 20 种文件类型，支持自定义扫描文件类型，支持常见的压缩格式文件扫描
		支持 400 万余种病毒的查杀，病毒库支持在线或者离线升级
安全平台及模块服务	售后服务	提供不少于两个月产品原厂商质保服务，承诺中标后提供原厂商授权和质保函。
		提供不少于两个月的原厂商上门 7x24 小时现场服务支持；
		原厂商在浙江省内有常驻机构能为用户提供快速及时的现场服务（须提供企业登记注册证明），提供本地应急响应时间<=4 小时；
		★项目实施人员须提供不少于 2 名中国信息安全测评中心认证的大数据安全分析师，提供证书复印件；

1.3.5 网络架构分析服务参数

为官网提供基于需要分析的整体网络或者目标区域网络的架构分析，详细服务范围如下：

- 网络拓扑
- 网络协议
- 网络流量
- 网络设备

网络架构分析会对目标网络的网络现状、网络建设规范性、网络可靠性、网络边界安全、网络流量分析、网络通信安全、网络设备安全和网络安全管理这八个方面进行网络架构安全性的全面分析，对整体网络中的脆弱点进行识别，评估结果包括定性和定量分析，让招标人对网络中存在的风险了如指掌。

交付物：《官网网络架构分析报告》

1.3.6 应急响应服务参数

应急响应服务主要面向官网提供已发生安全事件的事中、事后的取证、分析及提供解决方案等工作。

可以帮助官网完成下列类型安全事件的应急响应支持：

- 应用服务瘫痪问题
- 网络阻塞、DDoS 攻击问题
- 服务器遭劫持问题
- 系统异常宕机问题
- 恶意入侵、黑客攻击问题
- 病毒爆发问题
- 内部安全事故

根据服务地点，可以分为现场服务和远程服务两种。

- 现场服务：指接到紧急服务请求，支持人员在最短时间内赶赴采购人现场，协助分析事件可能的原因，解决各类安全事件。
- 远程服务：指通过电话、QQ 远程协助、远程临时接入等非现场的活动，协助分析事件可能的原因，解决各类安全事件。

交付物：

《安全事件应急响应分析总结报告》

1.3.7 安全漏洞评估服务参数

提供包括网络设备、操作系统、数据库、常见应用服务器以及 Web 应用等范围的扫描。

漏洞扫描的详细服务范围如下：

- 操作系统

Windows、发行版 Linux、AIX、UNIX 通用、Solaris、FreeBSD、HP-UX、BSD 等主流操作系统。

- 数据库

Oracle、MySQL、MSSQL、Sybase、DB2、Informix 等主流数据库。

- 常见应用服务

Apache、IIS、Tomcat、Weblogic 等主流应用服务，常见 FTP、EMAIL、DNS、TELENT、POP3、SNMP、SMTP、Proxy、RPC 服务等。

- Web 应用程序

ASP、PHP、JSP、.NET、Perl、Python、Shell 等语言编写的 WEB 应用程序。

- 网络设备

常见的路由器、交换机等设备。

交付物：

《操作系统安全漏洞扫描报告》

《数据库安全漏洞扫描报告》

《中间件安全漏洞扫描报告》

《网络设备安全漏洞扫描报告》

1.3.8 安全配置评估服务参数

安全配置检查服务范围包括各种网络设备、安全设备、主机操作系统、数据库、常见中间件及网络服务应用等。

安全配置检查的服务内容主要集中在设备的账号管理、口令管理、认证授权、日志配置、进程服务、外部端口等几个方面，覆盖了与安全问题相关的各个层面。

安全配置检查服务的针对不同系统的具体检查内容如下：

1) 网络设备安全配置检查包含但不限于以下内容：

- OS 安全
- 帐号和口令管理
- 认证和授权策略
- 网络与服务
- 访问控制策略
- 通讯协议、路由协议
- 日志审核策略
- 加密管理
- 设备其他安全配置

2) 主机操作系统安全配置检查包含但不限于以下内容：

- 系统漏洞补丁管理
- 帐号和口令管理
- 认证、授权策略
- 网络与服务、进程和启动
- 文件系统权限
- 访问控制
- 通讯协议
- 日志审核功能
- 防 DDOS 攻击
- 剩余信息保护
- 其他安全配置

3) 数据库安全配置检查包含但不限于以下内容：

- 漏洞补丁管理

- 帐号和口令管理
- 认证、授权策略
- 访问控制
- 通讯协议
- 日志审核功能
- 其他安全配置

4) 中间件及常见网络服务安全配置检查包含但不限于以下内容：

- 漏洞补丁管理
- 帐号和口令管理
- 认证、授权策略
- 通讯协议
- 日志审核功能
- 其他安全配置

交付物：

《操作系统安全配置核查报告》

《数据库安全配置核查报告》

《中间件安全配置核查报告》

《网络设备安全配置核查报告》

1.3.9 协助安全加固服务参数

安全加固服务范围包括各种网络设备、安全设备、主机操作系统、数据库、常见中间件及网络服务应用等。

安全加固前需提出系统的安全加固方案，在加固过程中可能产生对系统的不同程度、不同方面的影响，因此，安全加固的方案内容需综合考虑实际情况，针对不同的风险选择不同的策略。安全加固服务内容如下：

1) 网络设备安全加固包含但不限于以下内容：

- OS 升级
- 帐号和口令管理
- 认证和授权策略调整
- 网络与服务加固
- 访问控制策略增强
- 通讯协议、路由协议加固
- 日志审核策略增强
- 加密管理加固
- 设备其他安全配置增强

2) 主机操作系统安全加固包含但不限于以下内容：

- 系统漏洞补丁管理

- 帐号和口令管理
- 认证、授权策略调整
- 网络与服务、进程和启动加固
- 文件系统权限增强
- 访问控制管理
- 通讯协议加固
- 日志审核功能增强
- 防 DDOS 攻击增强
- 剩余信息保护
- 其他安全配置增强

3) 数据库安全加固包含但不限于以下内容：

- 漏洞补丁管理
- 帐号和口令管理
- 认证、授权策略调整
- 访问控制管理
- 通讯协议加固
- 日志审核功能增强
- 其他安全配置增强

4) 中间件及常见网络服务安全加固包含但不限于以下内容：

- 漏洞补丁管理
- 帐号和口令管理
- 认证、授权策略调整
- 通讯协议加固
- 日志审核功能增强
- 其他安全配置增强

交付物：

《操作系统安全加固建议报告》

《数据库安全加固建议报告》

《中间件安全加固建议报告》

《网络设备安全加固建议报告》

1.3.10 源代码安全审计服务参数

源代码审计服务的范围包括使用 ASP、ASP.NET（VB/C#）、JSP（JAVA）、PHP 等主流语言开发的 B/S 应用系统、使用 C++、JAVA、C#、VB 等主流语言开发的 C/S 应用系统，以及使用 XML 语言编写的文件、SQL 语言和数据库存储过程等。

评测需依据如下标准：

1、《GB/T22239-2008 信息安全技术 信息系统安全等级保护基本要求》；

2、《GB/T20984-2007 信息安全技术 信息安全风险评估规范》；

3、《GB/T18336.2-2015 信息技术 安全技术 信息技术安全性评估准则 第 2 部分：安全功能要求》；

4、《ZY-R-13-2016 信息系统安全评测规范》。

交付物：

《源代码安全审计报告》

1.3.11 应急预案编制服务参数

建立健全应急响应组织以及预防、预警机制，针对信息系统特点和可能的突发性安全事件拟制规范的应急处理流程，落实物质条件、人力和技术支撑等保障措施，制定出规范、全面、体系化的应急预案。内容应包含制定相应应急响应组织、预防、预警机制、事件定义分类、应急响应程序、事件上报处理机制、后期处理机制等内容。

交付物：

《安全事件应急响应预案》

1.3.12 安全配置策略定制服务参数

根据官网系统的业务的特定、提供的服务、开放的应用，以及整体系统的网络环境，结合相关标准要求，协助梳理、完善安全策略。定制化提出安全防护配置策略，开放仅需应用服务，加强安全访问控制，封闭不必要的危险服务和网络。

交付物：

《安全配置策略加固建议》

《安全配置策略加固报告》

1.3.13 恶意样本分析服务参数

针对恶意代码，提供分析服务，详细内容如下：

- ■ 操作系统排查包括：
- ✓ 可疑账号排查（隐藏、克隆账号）
- ✓ 可疑文件排查
- ✓ 可疑进程排查
- ✓ 可疑网络连接排查
- ✓ Rootkit 排查
- ■ 应用程序排查包括：
- ✓ WebShell 网页后门排查
- ✓ 一句话网页木马排查
- ✓ 数据库 JS 挂马排查
- ✓ 恶意插件排查
- ✓ 流氓软件排查

交付物：

《恶意样本分析报告》

1.3.14 安全演练设计服务参数

安全应急演练服务的对象范围主要针对组织核心业务及支撑核心业务的资源、人员、组织、流程、场所，以及相关第三方单位、上下级单位等，在服务过程中，重点需要梳理和掌握单位的组织架构、人员情况、业务流程、相关资产、关联第三方以及与应急演练相关的文档等。

交付物：

《安全演练方案》

《安全事件应急响应预案》

《安全演练总结报告》

1.3.15 安全渗透测试服务参数

经过由官网或公安机关相关网络安全监管部门授权，针对官网涉及的信息资产提供渗透测试服务，包括了操作系统、应用系统、WEB 程序和网络设备。

- 操作系统包括：

  Windows、发行版 Linux、AIX、Solaris、FreeBSD 等主流系统。

- 应用系统包括：

  Oracle、MySQL、MSSQL、Sybase、DB2、Informix 等主流数据库，Apache、IIS、Tomcat、Weblogic 等主流 WEB 服务器，FTP、DNS 等主流应用服务器。

- WEB 程序包括：

  ASP、PHP、JSP、.NET、Perl、Python、Shell 等语言编写的 WEB 程序。

- 网络设备包括：

  常见厂商的路由器、交换机等设备。

交付物：

《渗透测试报告》

1.3.16 主动诱捕服务参数

针对官网系统，提供主动诱捕服务，涉及服务包括：

- 模拟 Ssh 弱口令
- 模拟 IDS 设备
- 模拟工控系统
- 模拟 bash 漏洞
- 模拟 Web 文件包含漏洞
- 模拟低版本 Wordpress
- 模拟高危端口
- 模拟虚拟的服务器
- 模拟 WiFi

交付物：

《主动诱捕技术分析报告》

《应用系统威胁情报分析报告》

1.3.17 可信众测服务参数

可信众测采取远程漏洞挖掘的方式进行服务，服务范围包含但不仅限于 Web 应用系统安全测试、手机移动采购人端安全测试、嵌入式设备（含智能设备）安全测试。通过在签署保密协议授权组织不少于二十名可信黑帽子发起对官网应用系统的攻击，并通过审计及制定地点开放的方式进行入侵测试。

交付物：

《应用系统安全测试报告》

1.3.18 移动APP安全测试服务参数

移动 APP 安全测试应通过各种方法全面发现 APP 程序自身的安全漏洞，以人工检测为主，各类扫描工具为辅，在保证整个安全检测过程在可以控制和调整的范围之内尽可能地获取程序的安全隐患。通过将程序在模拟器或真实设备中，并结合前面收集的信息，动态调试程序可能存在的漏洞。

- **安全测试种类**

在移动端主流操作系统进行了深入的安全研究，包括 iOS 系统和 Android 系统。

Android 系统 APP 程序的安全测试包括如下内容：

1）使用工具对 APP 程序进行自动化扫描，对吸费、暗跑流量等恶意行为进行识别；

2）对 apk 文件进行反编译分析，测试 apk 文件是否被植入恶意代码等。

iOS 系统 APP 程序的安全测试包括如下内容：

1）使用工具对 APP 程序进行全面渗透测试；

2）对 APP 程序进行黑盒测试，检测不安全存储及内部通讯组件漏洞；

3）从 APP 客户端到服务器端进行安全检测。

交付物：

《Android APP 安全测试报告》

《IOS APP 安全测试报告》

1.3.19 定制安全通告服务参数

提供及时、准确的安全风险预警，第一时间通知采购人，并提供专业的安全解决建议。安全通告对象范围如下：

- 常见厂商的软、硬件网络设备：思科、华为等路由、交换设备；

- 常见厂商的操作系统：微软、惠普、苹果、IBM 等操作系统；
- 常见厂商的数据库软件：微软 MSSQL、甲骨文 Oracle 等；
- 常见厂商的 Web 软件：BEA Weblogic、IBM Websphere、Apache、JBoss、Tomcat 等。

安全通告提供最新安全漏洞、威胁（0day、系统漏洞、网络攻击）的解决办法、安全问题描述和相应的处理意见，及时提供符合官网实际需求的安全信息。安全通告服务具体内容由以下模块组成：

- 公告 ID：CVE 编号；
- 公告标题：漏洞名称；
- 厂商：漏洞涉及的厂商；
- 发布时间：漏洞发布时间；
- 受影响软件及系统：漏洞影响的软件及系统；
- 综述分析：对漏洞进行描述,同时分析其造成影响的原因；
- 解决方法：厂商补丁发布的链接；若厂商还未发布相应的补丁，根据安全问题的实际情况,提供暂时的解决方案。

交付物：《安全通告》周报

1.3.20 安全值守保障服务参数

现场值守服务的内容主要包括安全设备监控、安全巡检、安全日志分析、应急处置四项主要内容：

- 安全设备监控：对安全设备运行进行监控和维护；
- 安全巡检：对安全设备进行健康状态检查，包括系统引擎、CPU 占用率、内存占用率、接口状态、证书授权状态等内容；
- 安全日志分析：对安全设备产生的高、中风险告警事件进行分析，包括事件类型分布、事件发展趋势、事件频率、源地址、目的地址等内容；
- 应急处置：对突发安全事件进行应急响应，阻止安全事件影响扩大，查找安全事件产生原因。

交付物：

《安全保障值守日报》

《安全保障值守周报》

《安全保障安全巡检报告》

1.3.21 日志安全分析服务参数

针对官网的以下信息资产，包括：

- Web 应用日志，包括 IIS、Apache、Apache Tomcat、Nginx 等；
- 操作系统日志，包括 Windows、Linux 系统日志、安全日志、应用日志等；
- 网络设备，包括路由器、交换机等日志；
- 网络安全设备，包括网络入侵检测系统、网络审计系统、上网行为管理系统等日志。

提供以下日志分析服务内容：

- 常见 Web 攻击行为，包括 XSS、SQLinj、暴力破解等；
- 操作系统可疑行为，包括关机、重启、增删账户等；

- 网络可疑行为，包括网络设备关机、重启、配置变更等；
- 安全设备监控告警行为，包括检测的攻击行为、设备自身可疑操作行为等。

交付物：

《安全日志分析报告》

1.3.22 安全运营服务参数

根据官网系统日常运行情况，汇总分析一系列安全防护、监测、预警等持续性的安全保障措施形成的安全威胁情报、态势感知、事件等，并根据安全状况及时采取对应响应处置和追溯，以确保信息系统安全防护措施的有效性及事件处置的及时性。

交付物：

《安全运营报告》

1.3.23 云资源参数

名称	配置	月份	单位	数量
云服务器 1	C P U：4 vCPU 内存：8 GB 内网带宽：1.5 Gbps 50 万 PPS 高效云盘：150G 系统盘 Linux CentOS7.3	3	月	2
云服务器 2	C P U：4 vCPU 内存：8 GB 内网带宽：1.5 Gbps 50 万 PPS 高效云盘：100G 系统盘 Windows Server 2012 64 位中文版系统	3	月	2
云服务 3	C P U：4 vCPU 内存：16 GB 内网带宽：1.5 Gbps 50 万 PPS 高效云盘：100G 系统盘 Windows Server 2012 64 位中文版系统	3	月	2
云服务器 4	C P U：4 vCPU 内存：8 GB 内网带宽：1.5 Gbps 公网带宽：5M 50 万 PPS 高效云盘：150G 系统盘 Linux CentOS7.3	3	月	2
云服务器 5	C P U：4 vCPU 内　　存：8 GB 内网带宽：1.5 Gbps 公网带宽：5M 50 万 PPS	2	月	1

	高效云盘：150G 系统盘 高效云盘：1T 高效云盘			
云服务器 6	C P U：4 vCPU 内存：8 GB 内网带宽：1.5 Gbps 50 万 PPS 高效云盘：150G 系统盘 高效云盘：1T 高效云盘	2	月	1
云数据库 Mongodb	CPU：8C 内存：16G 数据盘：100G 复制集模式	3	月	1
云数据库 Redis	内存：16G 连接数：20000 最大内网带宽：48M 主从模式	3	月	1
云数据库 MySQL	CPU ：4C 内存：8G 数据盘： 200G 高可用性：支持 主从模式	3	月	1
带宽	30M	3	月	1

1.3.24 云防篡改软件参数

指标项	技术要求	
基本要求	产品形态	软件
	支持的操作系统	Windows2000,2003,2008 32&64 位 Redhat,CentOS,SUSE,Asianux 等 32&64 位 UNIX 系列：AIX ,HP-UX,Solaris
	支持 WEB 服务器	IIS，apache java 系列(weblogic,websphere,tomcat,jboss 等) nginx
	管理方式	B/S 管理方式，支持 windows/linux 平台。 管理端支持主备模式部署
	核心技术	采用先进内核驱动、WEB 核心内嵌和实时触发机制结合
防篡改功能	文件保护	支持各类网页文件的保护，包括静态和动态网页以及各类文件信息
	目录保护	支持对指定文件夹以及子文件夹的保护，避免上传非法文件及木马等恶意文件或插入恶意代码

	模板配置	支持在同一种操作系统下，网站路径相同，可通过规则模板，用模板统一将规则下发到各监控端，无需对监控端进行一一配置
	一键启停文件保护	一键启停所有监控端对文件保护，不必登录 WEB 服务器进行停启。
	断线检测和防护	在与其它模块网络断开的情况下能防止文件被篡改
	许可策略	支持基于目录、进程、文件、文件类型等进行设置许可。 支持正则表达式设置许可策略。 支持对符合许可策略的更新发布进行审计。
	自我保护	防篡改程序的进程被 kill，防篡改功能不会失效。 防篡改程序有自我保护机制。
防攻击功能	WEB 安全防护	能够有效防止 SQL 注入攻击、跨站攻击、溢出代码攻击、对危险文件类型的访问、对危险系统路径的访问、特殊字符构成的 URL 利用、防止构造危险的 Cookie 等。
	防字段溢出	支持自定义 HTTP 头的各字段溢出自定义
	规则自定义	支持防护规则基于 HTTP 头的各字段进行自定义
	基于时间，IP 调整规则	能根据时间段，IP 段进行规则调整。
同步功能	自动同步	支持事件触发机制和时间触发机制，将更新的文件同步到 WEB 服务器上。 且支持一对多同步。
	HA 功能	同步服务器自带 HA 功能，保证同步服务器高可用。
	增量同步	同步机制采用增量同步机制
	同步规则	支持同步规则自定义
管理控制	站点管理	对 WEB 状态监控，启动、停止等操作； 对 WEB 服务器的 CPU,内存，磁盘等信息进行监控展显。
	用户管理	支持多用户分级管理 管理端支持 ACL,设定允许的源 IP 才能访问
	日志	支持多种日志级别，并支持日志导出。 相同日志支持归并展现。
	告警方式	支持 SYSLOG、邮件、短信、界面提示等多种告警方式
	网站备份	支持对网站全量备份、增量备份和恢复。
性能指标	最大保护对象	不限

	最大保护深度	不限
	占用资源情况	CPU，内存占用资小于 3%

1.3.25 云堡垒机参数

服务项	技术要求
★操作审计	1.1 运维操作记录 操作失误、恶意操作、越权操作详细记录 1.2 linux 命令审计 可提取命令字符审计，命令定点回放 1.3 windows 操作录像 远程桌面的操作，全程录像，包括：键盘操作、鼠标操作、窗口打开等 1.4. 文件传输审计 支持远程桌面文件传输、SFTP 的原文件审计
职权管控	1.5. 账号管控 运维账号唯一性，解决共享账号、临时账号、滥用权限等问题 1.6. 权组管理 按照人员、服务器、服务器组，建立人员职责与资源分配的授权管理
★安全认证	1.7. 账号双因子认证 支持多种双因子认证机制，通过短信认证、RAM 子账号 MFA 等技术，控制账号密码泄露风险
高效运维	1.8. C/S 架构运维接入 支持 SSH、RDP、SFTP 协议 1.9. 支持各种运维工具 PuTTY、SecureCRT、Xshell、WinSCP、mstsc 等 1.10. ECS 高效接入 一键同步并导入云服务器 ECS

1.3.26 云主机安全参数

服务项	技术要求
主机漏洞检测和修复	1.1 系统软件 CVE 漏洞 通过检测服务器上安装软件的版本信息，与 CVE 官方的漏洞库进行匹

	配，检测出存在漏洞的软件并给您推送漏洞信息（可检测如：SSH、OpenSSL、Mysql 等软件漏洞） 1.2 Windows 系统漏洞 通过订阅微软官方更新源，若发现您服务器存在高危的官方漏洞未修复，将为您推送微软官方补丁（如“SMB 远程执行漏洞”，另外系统将只推送高危漏洞，安全更新和低危漏洞需要您手动更新） 1.3 Web-CMS 漏洞 共享阿里云安全情报源，通过目录及文件的检测方案，检出 Web-CMS 软件漏洞，并给您提供云盾自研补丁（可修复如：Wordpress、Discuz 等软件漏洞） 1.4 其他高危漏洞 可检测出配置型、组件型的漏洞，无法通过版本匹配和文件判断的漏洞（如：redis 未授权访问漏洞等）
高危配置基线核查	1.1 账户安全检测 深度检测服务器上是否存在黑客入侵后，留下的账户，对影子账户、隐藏账户、克隆账户进行提醒 1.2 弱口令检查 收集了常用的弱口令字典，检测您 SSH、RDP 等服务是否使用了弱密码 1.3 配置风险检测 对常见登录配置、进程配置、注册表配置进行检查，以达到企业级服务器安全准入标准
黑客入侵检测（含病毒云查杀）	1.1 异地登录提醒 记录所有登录记录，对于非常用登录的行为进行实时提醒，可自由配置常用登录地 1.2 暴力破解联动 对非法破解密码的行为进行识别，并上报到阿里云处罚中心进行拦截，避免被黑客多次猜解密码而入侵 1.3 网站后门查杀 自研网站后门查杀引擎，拥有本地查杀加云查杀体系，同时兼有定时查杀和实时防护扫描策略，支持常见的 php、jsp 等后门文件类型 1.4 主机异常检测 对反弹 Shell、对外 DDoS、挖矿等恶意进程，以及 C&C 肉鸡检测、恶意

	源下载等异常连接进行实时检测和告警 1.5　病毒云查杀 对接国内外主流云查杀引擎,同时自研沙箱,可检测出恶意进程及软件,并提供一键隔离功能
主机端口/进程/账号清点管理	1.1　资产清点 定期获取并记录服务器上运行的进程（对外监听端口、创建的账号）信息，进行统一的管理和清点 1.2　变动审计 对进程（监听端口、账号）的变动情况进行记录，便于审计历史变动，自主发现异常资产行为
主机全量日志实时检索	1.1　集中管理 类型包括：进程启动、网络连接、登录流水、账号信息、端口监听信息、全量进程信息 1.2　快速检索 支持逻辑（布尔表达式）检索，秒级展示，主机遇到问题时，可一站式搜索定位问题根源

1.3.27 云日志审计参数

技术指标	技术要求
规格	软件
处理性能	支持审计 20 个日志源。
日志收集	支持 Syslog、SNMP Trap、OPSec、FTP 协议日志收集; 支持使用代理(Agent)方式提取日志并收集; 支持目前主流的网络安全设备、交换设备、路由设备、操作系统、应用系统等; 设备厂家包括但不限于：Cisco(思科)，Juniper，联想网御/网御神州，F5，华为，H3C，微软，绿盟，飞塔(fortinet)，Foundry，天融信，启明星辰，天网，趋势，东软，Nokia，CheckPoint，Hillstone(山石)，安恒，珠海伟思，BEA，中国电信，安氏，帕拉迪，apc，arbor，clam，戴尔（dell)，digium，东方电子，EMC，中国电力科学研究院，Eudora，google，冠群金辰，linksys，Mcafee，netapp，NAS（美国国家安全局)，永达，sonicwall，vigor，天存，西岭，Symantec（赛门铁克)，Hardened-PHP，foundertech(方正)，三零盛安，allot，蓝盾，IBM，金诺网安，网威，nortel(北电)，citrix(思杰)，watchguard，中兴，

	阿帕奇，WINDOWS 系统日志，Linux/UNIX syslog、IIS、Apache 等； 支持常见的虚拟机环境日志收集，包括 Xen、VMWare、Hyper-V 等。
日志分析	可以以日志等级进行过滤； 应该可以通过自定义配置将用户不关心的日志过滤掉； 支持对收集到的重复的日志进行自动的聚合归并，减少日志量； 支持可由用户定义和修改的日志的聚合归并逻辑规则； 支持将收集到的日志转发，当原始日志设备无法设置多个日志服务器时，可以通过本系统的日志转发功能将日志转发到其他日志存储设备； 支持对收集到的日志进行解析（标准化、归一化），解析规则可以根据客户要求定制扩展； 可对日志进行细粒度解析，解析后的日志根据具体日志包含但不限于：日期、发生时间、接收时间、设备类型、日志类型、日志来源、威胁值、源地址、目的地址、事件类型、时间范围、操作主体、操作对象、行为方式、技术动作、技术效果、攻击类型、特征类型、协议、地理信息（公网情况）； 支持基于内存的实时关联分析，跨设备的多事件关联分析； 支持自定义条件的事件进行聚合； 具备安全评估模型，评估模型基于设备故障、认证登陆、攻击威胁、可用性、系统脆弱性等纬度加权平均计算总体安全指数。安全评估模型可以显示总体评分、历史评分趋势。安全评估模型各项指标可钻取具体的评分扣分事件。 内置非法访问、可疑入侵、病毒爆发、设备异常、弱点针对等 5 大类 50 子类的安全分析场景 进行关联分析的规则可定制；
★关联分析	系统须具备一个安全知识库和包含资产信息的弱点库，当接收到指定资产并且匹配到弱点库中指定漏洞的攻击时，须触发与安全知识库、弱点库的关联，新增新的事件，并且提高威胁等级。需提供第三方权威测评机构（必须是公安部三所、国家保密局、ISCCC 其中一家）的功能检测报告。
日志备份	可设置日志存储备份策略。包括系统日志保存期（天）、磁盘使用率百分比； 支持日志备份自动传送到远程服务器；
日志查询	支持 B/S 模式管理，支持 SSL 加密模式访问；

	支持按日期、时间、设备类型、日志类型、日志来源、威胁值、源地址、目的地址、事件类型、时间范围、操作对象、技术方式、技术动作、技术效果、攻击类型、地理城市等参数进行过滤查询； 支持用任意关键字对所有事件进行高性能全文检索； 支持可指定多个查询条件进行组合查询； 支持将查询的条件存储为查询模版，方便再次使用； 极高的日志高查询性能，支持亿级的日志里根据做任意的关键字及其它的检索条件，在秒级里返回查询结果。
★应用性能监控	性能监控:通过在目标主机上安装 agent 程序,支持监控目标主机的 CPU 利用率、内存使用率、磁盘使用情况、流量等信息，并支持设置报警阈值。需提供第三方测评机构（必须是公安部三所、国家保密局、ISCCC 其中一家）的检测报告
告警功能	可预设置安全告警策略； 支持数据阀值设置，超过阀值将产生告警； 可以通过邮件、短信和屏幕显示进行告警； 支持自动防止报警信息在短时间内大量发送(告警抑制)； 具备报警合并和在一个时间段内抑制报警次数的能力。
综合查询及报表管理	内置合规性报表 1000+种； 内置 SOX、ISO27001、WEB 安全等解决方案包； 内置完善的等级保护合规报表； 内置综合性自动化审计报告； 支持用户自定义报表； 自定义的报表支持多个统计维度的数据集合； 支持报表导出为 PDF 和 Word 格式文件。
用户管理	根据三权分立的原则和要求进行职、权分离，对系统本身进行分角色定义，如管理员只负责完成设备的初始配置，规则配置员只负责审计规则的建立，审计员只负责查看相关的审计结果及告警内容；日志员只负责完成对系统本身的用户操作日志管理； 系统自带自身管理日志；

1.3.28 云数据库审计参数

服务项	技术要求

★用户审计	关联应用层和数据库层的访问操作 可溯源到应用者的身份和行为
多角度线索	风险和危害线索：高中低的风险等级、SQL 注入、黑名单语句、违反授权策略的 SQL 行为 会话线索：根据时间、用户、IP、应用程序、和客户端多角度分析 详细语句线索：提供用户、IP、客户端工具、访问时间、操作对象、SQL 操作类型、成功与否、访问时长、影响行数等多种检索条件
★实时告警	异常操作风险：通过 IP、用户、数据库客户端工具、时间、敏感对象、返回行数、系统对象、高危操作等多种元素细粒度定义要求监控的风险访问行为 SQL 注入：系统提供了系统性的 SQL 注入库，以及基于正则表达式或语法抽象的 SQL 注入描述，发现异常立即告警 黑白名单：提供准确而抽象的方式，对系统中的特定访问 SQL 语句进行描述，使这些 SQL 语句出现时能够迅速报警
详尽报表	会话行为：登录失败报表、会话分析报表 SQL 行为：新型 SQL 报表、SQL 语句执行历史报表、失败 SQL 报表 风险行为：告警报表、通知报表、SQL 注入报表、批量数据访问行为报表 政策性报表： 塞班斯报表

三、 商务要求：

（1）**服务时间：**官网安全防护服务：自合同签订日起，持续两年；

大会期间重保服务：自合同签订日起，至 2018 年 12 月 31 日。

（2）付款方式：待首届联合国世界地理信息大会重保服务完成且官网安全防护平台审核通过后，一次性付清

（3）若成交供应商为浙江省外公司，则须承诺签订合同前在湖州地区设立办事处。

第四章 磋商原则和程序

一、拆封采购响应文件

（一） 需方在竞争性磋商文件规定的时间和地点进行竞争性磋商，磋商响应方授权代表必须参加。参加磋商会的磋商响应方法定代表人或其授权代理人应出具其有效身份证明等，磋商响应方的法定代表人或其授权代理人未参加磋商会或迟到的，事后不得对采购相关人员、磋商过程和磋商结果提出异议；

（二） 磋商开始时，将查验采购响应文件密封情况，确认无误后拆封采购响应文件。

二、磋商小组

（一） 磋商小组依法由 3 人组成，其成员由采购方代表及从政府采购评审的相关专家库中通过随机方式抽取的专家组成，磋商小组对采购响应文件进行审查、质疑、评估和比较。

（二） 磋商期间，磋商响应方法人代表或法人委托人必须在场，负责解答有关事宜。

三、竞争性磋商评审原则与方法

（一）磋商小组将遵循公开、公平、公正，科学合理，竞争择优的原则，对磋商响应方提供项目方案与磋商文件的响应情况、人员配备情况、综合实力情况、服务网点情况、项目业绩、政策分、投标书编制质量等进行综合分析考评，由磋商小组根据综合评分法确定成交供应商。

（二）客观、公正的对待所有磋商响应方，对所有磋商评价，均采用相同的程序和标准。

（三）磋商会开始后，直至授予成交供应商合同为止，凡属于对采购响应文件的审查、澄清、评判和比较的有关资料、成交候选供应商的推荐情况及与磋商有关的其他任何情况均依法严格保密。

（四）磋商小组分别与各磋商响应方进行商务、技术磋商，在磋商过程中磋商小组成员不得透露其他磋商响应方的磋商信息，严守商业秘密。

（五）在磋商期间，磋商响应方不得向磋商小组成员询问磋商情况，不得进行旨在影响磋商结果的活动，否则将废除其磋商资格，并不再返还磋商保证金。

（六）在磋商过程中，磋商小组成员不得与磋商响应方私下交换意见，在竞争性磋商工作结束后，凡与磋商情况有接触的人不得将磋商情况扩散出磋商小组成员之外。

（七）需方不向落标方解释落标原因，不退还采购响应文件。

四、磋商程序

（一） 磋商会由采购代理机构主持，主持人宣布磋商会议开始。

（二） 主持人介绍参加磋商会的人员名单。

（三） 主持人宣布磋商期间的有关事项，告知应当回避的情形,提请有关人员回避。

（四） 磋商供应商推选代表检查磋商响应文件密封的完整性并签字确认。

（五） 经确认无误后打开资信商务文件、技术文件和初次报价文件外包装，清点磋商响应文件正本、副本数量，将符合采购文件要求的送评标室审核。

（六） 磋商小组确认采购文件，讨论决定是否需要求采购文件的要求（采购文件规定的可变动部分）进行实质性变动。

（七） 采购人或代理机构检查磋商响应方提交的资格证明文件，对磋商响应方进行资格审查。

（八） 磋商小组审核采购响应文件。

A. 磋商小组按照商务、技术等进行分工审核采购响应文件。各专家在全面审核的基础上有侧重的进行分工。

B. 依据竞争性磋商文件的规定，从采购响应文件的有效性、完整性和对竞争性磋商文件的响应程度进行审查，以确定是否对磋商文件的实质性要求作出响应。

（九） 磋商小组汇总并讨论审核情况，确定磋商响应方是否具有磋商资格。

（十） 在磋商过程中，磋商小组可以根据磋商文件和磋商情况实质性变动采购需求中的技术、服务要求以及合同草案条款，但不得变动磋商文件中的其他内容。实质性变动的内容，须经采购人代表确认。（对磋商文件作出的实质性变动是磋商文件的有效组成部分，磋商小组应当及时以书面形式同时通知所有参加磋商的供应商。）

（十一） 供应商按照磋商文件的变动情况和磋商小组的要求重新提交响应文件，并由其法定代表人或授权代表签字或者加盖公章。由授权代表签字的，应当附法定代表人授权书。供应商为自然人的，应当由本人签字并附身份证明。

（十二） 采购响应文件的澄清。

为有助于采购响应文件的审查、评判和比较，磋商小组可以书面形式要求磋商响应方对采购响应文件含义不明确的内容作必要的澄清或说明，磋商响应方应采用书面形式进行澄清、说明或承诺。磋商响应方对磋商中所涉及的澄清、修改、承诺等补充资料等在规定的时间内以书面文件形式提交至磋商小组，其书面文件必须由磋商响应方的法定代表人或其授权代理人签字（或签章），作为采购响应文件的补充。如该磋商响应方成为成交供应商，则该磋商响应方的采购响应文件（含所有补充资料）将作为合同的组成部分。

（十三） 对响应文件初次报价部分进行磋商，要求供应商剔除初次报价中不合理的成分。

（十四）各磋商响应方在本项目全部磋商结束后进行最终报价，磋商小组对最终报价的合理性进行审核**（最终报价不得高于初次报价，否则为无效报价）。**磋商小组根据评标内容及标准对提交最终报价的供应商的响应文件和最后报价进行综合评分。

（十五）起草评审报告，所有磋商专家须在评审报告上签字确认。

（十六）本项目由采购人（或采购人事先授权磋商小组）按照磋商报告中推荐的排列顺序依法确定成交供应商。

五、采购响应文件计算错误的修正

A.采购响应文件中磋商报价一览表内容与采购响应文件中磋商分项报价表内容不一致的，以磋商报价一览表为准；

B.采购响应文件的大写金额和小写金额不一致的，以大写金额为准；

C.总价金额与按单价汇总金额不一致的，以单价金额计算结果为准；

D.单价金额小数点有明显错位的，应以总价为准，并修改单价；

E.对不同文字文本采购响应文件的解释发生异议的，以中文文本为准。

六、综合评分法

为公正、公平、科学地选择中标人，根据《中华人民共和国政府采购法》等有关法律法规的规定，并结合本项目的实际，制定本办法。

本办法适用于德清县公安局首届联合国世界地理信息大会官网安全防护项目的评标。

6.1 总则

本次评标采用综合评分法，总分为100分，其中价格分、商务资信分、技术分三部分。合格磋商响应供应商的评标得分为各项目汇总得分，中标候选资格按评标得分由高到低顺序排列，得分相同的，按投标报价由低到高顺序排列,得分且投标报价相同的，按技术得分由高到低顺序排列。评分过程中采用四舍五入法，并保留小数2位。

磋商响应供应商评标综合得分=价格分+(技术分+商务资信分)

磋商小组认为竞标人的报价明显低于其他通过符合性审查竞标人的报价,有可能影响产品质量或者不能诚信履约的，应当要求竞标人书面说明（包括货物的进货或主要原材料、部件成本，人工成本和合理利润等多种构成要素说明），必要时要求提供相关证明材料（可以传真的形式当场提供,但必须在事后提供相应的原件进行核实）。竞标人不能在磋商小组提出说明要求后半小时内当场合理说明原因并提供证明材料的,磋商小组应将该竞标人的投标文件作无效处理，并在评审报告中说明。

二分之一以上的评委认为供应商报价明显高于市场平均价的将作为无效竞标处理。

6.2 评标内容及标准

评分项目	分值	评标要点及说明
投标报价	10	满足招标文件要求（实质性响应）且投标报价最低的为评标基准价，其价格分为满分。其他投标人的价格分统一按照下列公式计算：投标报价得分=（评标基准价/投标报价）*10(百分点保留2位小数点，得分保留2位小数,第3位四舍五入,下同)。

评分项目	分值	评标要点及说明
技术部分60分	47	**项目方案与磋商文件的响应情况** 1、根据响应方所提供的技术参数偏离情况进行打分，满分27分，打★的技术项为需求配置功能，一项不满足扣3分，6项以上（不含6项）不满足，此项得0分，其他负偏离每项扣1分，扣完为止； 2、根据响应方提供的官网加固方案的完整程度进行打分，方案完整的得2.1-3分，方案良好的得1.1-2分，方案一般的得0.5-1分； 3、响应方需充分考察并了解大会官网相关情况，并根据考察结果提供大会官网的《网络架构拓扑图》、《服务器配置清单》、《系统功能示意图》，根据响应方提供文档的完整及相符情况进行打分，每项最高得2分，总分不超过6分； 4、响应方需根据大会官网现状提出有关网站加固的建设性意见，每条得1分，最高得3分； 5、响应方提供的备份节点机房为自身所有，即提供的增值电信业务经营许可证（因特网数据中心业务）与响应方名称一致的得2分，许可证名称与响应方名称不一致的，此项不得分。 6、响应方所提供的备份节点机房需具备多线带宽接入的能力，每接入一个运营商（仅限电信、联通、移动）线路的得2分，总分不超过6分，需提供线路接入相关证明材料。
	13	**人员配备情况** 1、响应方每提供一个具有CCNP/HCNP/H3CNE证书工程师的得1分；每提供一个具有CCIE,HCIE,H3CIE证书工程师的得2分，总得分不超过3分，需提供证书复印件，且证书持有人在响应方单位缴纳一年以上社保证明文件并加盖公章。 2、响应方每提供一个具有PMP人员证书的得2分，最高得4分，需提供证书复印件及证书持有人一年以上社保证明文件并加盖公章。 3、响应方每提供一个具有CISP人员证书的得2分，最高得6分，需提供证书复印件及证书持有人一年以上社保证明文件并加盖公章。

评分项目	分值	评标要点及说明
资信及商务部分30分	13	**综合实力情况** 1、响应方具有 CMMI3 级别证书的得 1 分，具有 CMMI5 证书的得 2 分，总分不超过 2 分，如不提供证书复印件不得分； 2、响应方具有 ISO27001 证书的得 2 分，如不提供证书复印件不得分； 3、响应方具有工商企业信用 AA 级“守合同重信用”荣誉证书的得 1 分，具有工商企业信用 AAA 级“守合同重信用”荣誉证书的得 2 分，总分不超过 2 分，必须提供证书复印件或工商网上截图并加盖公章，否则不得分； 4、响应方获得由市级及以上公安机关网警部门（网络与信息安全信息通报中心）颁发的网络安全先进单位的，每提供一份得 1 分，总分不超过 2 分，如不提供证书复印件不得分； 5、企业信用：经“信用中国”网站（www.creditchina.gov.cn）查询，竞标人具有守信红名单记录的，得 2 分（以该网站截图盖章为准，否则不予计分）； 6、截止开标时间，不良行为仍在公告期内的，每出现一次扣 1 分；不良行为虽已在公告期外，但在三年内的，每出现一次扣 0.5 分；不良行为认定文书及公告中未注明公告期限的，每出现一次扣 0.2-0.5 分；未出现不良行为的得 3 分。
	6	**服务网点情况** 1、响应方的公司注册地和备份节点机房在湖州地区的得 3 分，在浙江省内其他地区得 2 分，在浙江省外得 1 分（提供公司全称、营业执照或租房协议、地址、联系人、联系方式等）。 2、响应方技术团队在湖州地区的且人数达到 6-20（含）人的得 2 分，20 人以上的得 3 分；响应方技术团队在浙江省其他地区的且人数达到 6-20（含）人的得 1 分，20 人以上的得 2 分。（需提供相关人员一年以上社保证明材料复印件加盖公章）

评分项目	分值	评标要点及说明
	8	**项目业绩** 1、响应方参与过重大活动（主办方为市级及以上单位）的官网防护工作的得 3 分，需提供合同复印件； 2、响应方有市级及以上重要安全平台（态势感知平台或云防护平台）建设及运营经验，其中安全平台需通过公安部检测并获得国家公安部计算机信息系统安全专用产品销售许可证及计算机软件著作权登记证书，如能提供相关证明材料的得 2 分，如不提供材料不得分； 3、响应方每提供一个与市级及以上政府或企业签订云防护或态势感知案例的得 0.5 分，总分不超过 3 分，案例需提供相关合同复印件，否则不得分。 注：以上合同或证明材料均需提供复印件加盖公章，原件备查。
	2	**政策分** 1.磋商响应方为中小企业的，且提供的货物或服务为本单位（或其他中小企业）制造或提供的，得 1 分。以提供中小企业声明函和相关政府部门证明为准。 2. 磋商响应方按规定享受其他国家政策支持、扶持的，得 1 分。（以提供的相关政府部门证明资料和法律依据为准）
	1	**投标书编制质量** 投标文件编排有序、装订整齐、书面整洁、内容完整详实的，得 1 分；投标文件内容不完整、资料不全、格式不规范、装订不整齐等酌情扣分，扣完为止。

6.3 技术、商务资信分的计算

技术、商务、资信及其他分按照评标委员会成员的独立评分结果汇总数的算术平均分计算，计算公式为：

技术商务资信分=评标委员会所有成员评分合计数/评标委员会组成人员数

七、废标

在采购中，出现下列情形之一的，应予废标（法律、法规、规章、省级及以上监管部门规定的其他情形除外）：

1.出现影响采购公正的违法、违规行为的；

2.因重大变故，采购任务取消的；

3.磋商响应方的报价均超采购预算的，采购人不能支付的。

八、成交通知

（一）磋商结束后，采购代理机构在浙江省政府采购网、德清县公共资源交易中心网发布成交结果公告，由采购代理机构签发《成交通知书》。**如有恶意质疑、投诉，且导致授予合同的期限延期的，将没收其磋商保证金，并将其列入不诚信供应商名单。情节严重的将直接进入政府采购黑名单。**

（二）除不可抗力等因素外，成交通知书发出后，采购人改变采购结果，或者成交供应商拒绝签订政府采购合同的，应当承担相应的法律责任。**拒绝签订政府采购合同的成交供应商不得参加对本项目重新开展的采购活动。**

（三）一旦被确定为中标（成交）候选供应商的，应在中标（成交）通知书发出前三个工作日内进行注册申请为注册政府采购供应商，否则，采购组织单位有权拒绝向其发出中标（成交）通知书，并直接推荐排名次之的供应商为中标（成交）候选供应商，以此类推。

九、合同授予

（一）采购人与成交供应商应当在《成交通知书》发出之日起 30 日内签订政府采购合同。同时，采购代理机构对合同内容进行审查，如发现与采购结果和磋商承诺内容不一致的，将予以纠正。

（二）**合同正本应一式四份，采购单位与供应商双方各执一份；其他两份交由代理机构。**

（三）成交供应商拖延、拒签合同的,将被扣罚磋商保证金并取消中标资格。

第五章 合同主要条款
（仅供参考）
浙江省政府采购合同指引（服务）

项目名称：　　项目编号：

甲方：（买方）

乙方：（卖方）

甲、乙双方根据____政府采购项目的采购结果，签署本合同。

一、服务内容：

二、合同金额：

2.1 本合同金额为（大写）：_____元（￥_____元）人民币。

三、技术资料

3.1乙方应按谈判文件规定的时间向甲方提供有关技术资料。

3.2 没有甲方事先书面同意，乙方不得将甲方提供的有关合同或任何合同条文、规格、计划、图纸、样品或资料提供给与履行本合同无关的任何其他人。即使向履行本合同有关的人员提供，也应注意保密并限于履行合同的必需范围。

四、知识产权

4.1 乙方应保证提供服务过程中不会侵犯任何第三方的知识产权。

六、履约保证金

6.1 乙方交纳人民币____元作为本合同的履约保证金。

七.转包或分包

7.1 本合同范围的货物，应由供方直接供应，不得转让他人供应；

7.2 除非得到需方的书面同意，供方不得部分分包给他人供应。需方有绝对权力阻止分包。

7.3 如有转让和未经需方同意的分包行为，需方有权给予终止合同。

八、服务质量保证期和服务质量保证金（注：选用）

8.1 服务质量保证期_____年。（自验收合格之日起计）

8.2 服务质量保证金_____元。（履约保证金在中标规划编制单位按合同约定验收合格后自行转为质保金）

九、合同履行时间、履行方式及履行地点

9.1 履行时间：

9.2 履行方式：

9.3 履行地点：

十、款项支付

10.1 付款方式：

十一、税费

11.1 本合同执行中相关的一切税费均由供方负担。

十二、质量保证及后续服务

12.1 乙方应按谈判文件规定向甲方提供服务。

12.2 乙方提供的服务成果在服务质量保证期内发生故障，乙方应负责免费提供后续服务。对达不到要求的，根据实际情况，经双方协商，可按以下办法处理：

⑴重做：由乙方承担所发生的全部费用。

⑵贬值处理：由甲乙双方合议定价。

⑶解除合同。

12.3 如在使用过程中发生问题，乙方在接到甲方通知后在_____小时内到达甲方现场。

12.4 在服务质量保证期内，乙方应对出现的质量及安全问题负责处理解决并承担一切费用。

十三、、违约责任

15.1 甲方无正当理由拒绝接受服务的，甲方向乙方偿付合同款项百分之五的违约金。

15.2 甲方无故逾期验收和办理款项支付手续的,甲方应按逾期付款总额每日万分之五向乙方支付违约金。

15.3 乙方逾期提供服务的，每日向甲方支付千分之六违约金。逾期超过约定日期10个工作日不能交货的，甲方可解除本合同。乙方因逾期交货或因其他违约行为导致甲方解除合同的，乙方应向甲方支付合同总值5%的违约金，如造成甲方损失超过违约金的，超出部分由乙方继续承担赔偿责任。

十四、不可抗力事件处理

16.1 在合同有效期内，任何一方因不可抗力事件导致不能履行合同，则合同履行期可延长，其延长期与不可抗力影响期相同。

16.2 不可抗力事件发生后，应立即通知对方，并寄送有关权威机构出具的证明。

16.3 不可抗力事件延续120天以上，双方应通过友好协商，确定是否继续履行合同。

十五、诉讼

17.1 双方在执行合同中所发生的一切争议，应通过协商解决。如协商不成，可向合同签订地法院起诉。

十六、合同生效及其它

18.1 合同经双方法定代表人或授权委托代理人签字并加盖单位公章后生效。

18.2合同执行中涉及采购资金和采购内容修改或补充的，须经财政部门审批，并签书面补充协议报政府采购监督管理部门备案，方可作为主合同不可分割的一部分。

18.3本合同未尽事宜，遵照《合同法》有关条文执行。

18.4 本合同正本一式两份，具有同等法律效力，甲乙双方各执一份；副本____份，(用途)。

甲方：　　乙方：

地址：　　地址：

法定代表人：　　法定代表人：

签订地点：　　签订日期：　　年　月　日

第六章 采购响应文件格式

本章节内容提供部分采购响应文件格式，采购文件中要求，但未提供格式的，须由磋商响应方自行制作。

附件一：

供应商市场行为信誉（信用）情况承诺书（申明书）

<table>
<tr><td colspan="2">投（竞）标供应商名称</td><td></td><td>企业资质等级

（如 有）</td><td></td></tr>
<tr><td colspan="2">企 业 地 址</td><td></td><td>联 系 电 话</td><td></td></tr>
<tr><td colspan="2">拟投（竞）标项目名称</td><td></td><td>拟投标项目负责人姓名及资质</td><td></td></tr>
<tr><td rowspan="4">供应商
市场
行为
信誉
情况</td><td>有无受到财政监管部门处理、公告的不良行为。（未注明公告期限的）</td><td colspan="3"></td></tr>
<tr><td>有无受到财政监管部门处理、公告的不良行为（在公告期内）。</td><td colspan="3"></td></tr>
<tr><td>有无受到财政监管部门处理、公告的不良行为（不在公告期但在三年内）。</td><td colspan="3"></td></tr>
<tr><td>申请报名前三年内，在经营活动中有无重大违法记录（重大违法记录包括：（一）县级以上行政机关对供应商或其法定代表人、董事、监事、高级管理人员在经营活动中的违法行为做出的行政处罚决定，但警告和罚款额在人民币一万元以下的行政处罚决定除外。（二）各级司法机关对供应商或其法定代表人、董事、监事、高级管理人员在经营活动中的违法行为做出的刑事判决。）</td><td colspan="3"></td></tr>
<tr><td>供应商
信用
情况</td><td>是否列入失信被执行人、重大税收违法案件当事人名单、政府采购严重违法失信行为记录名单及其他不符合《中华人民共和国政府采购法》第二十二条规定条件。</td><td colspan="3"></td></tr>
<tr><td colspan="2">投标供应商

声 明</td><td colspan="3">以上内容是本企业市场行为信誉（信用）的真实反映，如有不实，愿取消本项目投标资格。

法定代表人签名或盖私章：

(单位公章)

日 期： 年 月 日</td></tr>
</table>

注：1、本表格内容须如实填写；

2、本表格须在投标时作为投（竞）标文件的商务部分内容放入投（竞）标文件中；

3、本表格由供应商自己填写，若无表中所列情况，则在相应栏中写“无“，若有，须按具体次数分别说明（包括处罚时间、事由、处罚主体等）；

4、联合体成员存在不良信用记录的，视同联合体存在不良信用记录。

5、供应商对上述情况进行承诺同时可提供“信用中国”网站（www.creditchina.gov.cn）或中国政府采购网（www.ccgp.gov.cn）查询截图，无不良或受惩信用记录，并加盖公章；若磋商响应方未提供上述网站截图则在磋商时由采购人或采购代理机构查询作为资格证明材料（截图查询日期须在开标截止前两个星期内）。

“信用中国”网站（www.creditchina.gov.cn）或中国政府采购网（www.ccgp.gov.cn）查询截图黏贴处

附件二：

声 明 书

致：_____（招标机构、采购单位名称）：

_____（磋商响应方名称）系中华人民共和国合法企业，经营地址。

我____（姓名）系_____（磋商响应方名称）的法定代表人，我方愿意参加贵方组织的_____项目的磋商，为便于贵方公正、择优地确定中标人及其投标产品和服务，我方就本次投标有关事项郑重声明如下：

1.我方向贵方提交的所有磋商响应文件、资料都是准确的和真实的。

2.我方现已清楚知道本项目的采购人情况，与之不存在投资关系、行政隶属关系、业务指导关系以及其他可能影响采购公正性的厉害关系。（如有，请如实说明）

3.在获知本项目采购信息后，与采购人聘请的为此项目提供咨询服务的公司及其附属机构没有任何联系。（如有，请如实说明）

4.我方此次向贵方提供的产品名称为：

5.我方诚意提请贵方关注：近期有关该类服务的重大决策和事项有：

_____

_____

6.我方及由本人担任法定代表人的其他机构最近三年内被通报或者被处罚的违法行为有：

_____

_____

7.以上事项如有虚假或隐瞒，我方愿意承担一切后果，并不再寻求任何旨在减轻或免除法律责任的辩解。

法定代表人签字或盖私章：

磋商响应方公章： 年 月 日

附件三：

法定代表人授权委托书

致德清天勤会计师事务所有限责任公司 ：

本授权委托书声明：我（法定代表人姓名）系（投 标 人 名 称）的法定代表人，现授权委托（授权代表姓名）为我公司法定代表人授权代表，参加贵处组织的（采购项目名称，括号中填写项目编号）项目磋商，全权处理本次招磋商活动中的一切事宜，我承认授权代表全权代表我所签署的本项目的磋商文件的内容。

授权代表无转授权，特此授权

授权代表：（签字） 性别：_____ 年龄：_____职务：_____

详细通讯地址：_____ 邮政编码：_____

电话：_____ 传真：_____

磋商响应方：_____（盖章）

法定代表人：_____（亲笔签名或盖私章）

授权委托日期：_____年 ____月_____日

——————————————————————————————

被授权人有效身份证复印件粘贴处

附件四：

磋商响应方基本情况一览表

单位名称	
企业代码	
经营地址	
企业法人	
经济类型	
授权代表	
公司成立时间	
公司联系电话、传真	
职工总人数	
资产总额	
其中固定资产原值	
固定资产净值	
负债总额	
其中银行借款	
所有者权益总额	
其中实收资本	
上年工业总产值	
上年销售收入	
上年销售利润	

磋商响应方：_____（公章）

法定代表人或授权代表（签字）：_____

日期：_____年_____月_____日

附件五：

项目业绩表

采购项目名称：　　采购编号：

序号	业主方	合同金额	签订时间	业主联系人	联系方式

注：须提供磋商响应方的合同复印件、证明材料，原件备查

磋商响应方全称（加盖公章）：

法定代表人或授权代表（签字或盖章）：

日期：

附件六：

商务响应表

采购项目名称：　　采购编号：

序号	采购文件的商务条款	采购响应文件对应的商务条款	响应情况

注：本表格不填写视同完全响应采购文件要求，此表可在不改变格式的情况下自行制作。

磋商响应方全称（加盖公章）：

法定代表人或授权代表（签字或盖章）：

日期：

附件七：

中小企业声明函

本公司郑重声明，根据《政府采购促进中小企业发展暂行办法》（财库[2011]181 号）的规定，本公司为_____（请填写：中型、小型、微型）企业。即，本公司同时满足以下条件：

1.根据《工业和信息化部、国家统计局、国家发展和改革委员会、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）规定的划分标准，本公司为_____（请填写：中型、小型、微型）企业。

2.本公司参加_____单位的_____项目采购活动提供本企业制造的货物，由本企业承担工程、提供服务，或者提供其他_____（请填写：中型、小型、微型）企业制造的货物。本条所称货物不包括使用大型企业注册商标的货物。

本公司对上述声明的真实性负责。如有虚假，将依法承担相应责任。

企业名称（盖章）：

日期：

附件八：

中小企业资格确认意见书

根据《工业和信息化部、国家统计局、国家发展和改革委员会、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）规定的划分标准，兹确认　　公司为　　行业的　　（请填写：中型、小型、微型）企业。

政府部门盖章

附件九：

残疾人福利性单位声明函

本单位郑重声明，根据《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）的规定，本单位为符合条件的残疾人福利性单位，且本单位参加_____单位的_____项目采购活动提供本单位制造的货物（由本单位承担工程/提供服务），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）。

本单位对上述声明的真实性负责。如有虚假，将依法承担相应责任。

单位名称（盖章）：

日　期：

附件十：

技术和服务偏离说明表

采购项目名称：　　采购编号：

序 号	内容	采购文件规范要求	采购响应文件对应规范	偏离情况	备 注

注：本表格不填写视同完全响应采购文件要求。此表可在不改变格式的情况下自行制作

磋商响应方全称（加盖公章）：

法定代表人或授权代表（签字或盖章）：

日期：

附件十一：

采购响应函

致德清天勤会计师事务所有限责任公司 ：

（磋商响应方全称） 授权 （授权代表名称、职务、职称） 为本公司授权代表，参加贵方组织的（采购项目名称）（括号内填项目编号） 采购的有关活动，进行磋商。为此声明如下：

1、 按照采购文件要求制作并提交规定的采购响应文件正本一套，副本两套。

2、 本次磋商的总报价：人民币_____元整（￥_____元）。

项目负责人：_____；职务：_____；职称：_____；年龄：_____。

3、 保证遵守采购文件中的有关规定和收费标准。

4、 保证严格执行甲、乙双方所签的经济合同，并承担全部规定的责任义务。

5、 我方已详细审查“采购文件”的所有内容，包括澄清、修改文件（如果有）和所有已提供的参考资料以及有关附件，我方完全明白并认为此采购文件没有倾向性和排斥潜在磋商响应方的内容，也不存在引起歧义和误解的内容，已经了解我方对于采购文件、采购过程、采购结果有依法进行询问、质疑、投诉的权利及相关渠道和要求，所以我方同意采购文件的相关条款，放弃对采购文件提出误解和质疑的一切权力。

6、 我方在采购响应之前已经与贵方进行了充分的沟通，完全理解并接受采购文件的各项规定和要求，对采购文件的合理性、合法性不再有异议。

7、 愿意向贵方提供任何与该项磋商有关的数据、情况和技术资料，完全理解贵方不一定接受最低价的磋商。

8、 本采购响应文件对采购文件要求的偏离或保留均已在采购响应文件第___页，第___条中明示或在磋商偏离表中明示。

9、本采购响应文件自磋商之日起 90 个工作日内有效。

10、与本磋商有关的一切往来通讯请寄：

地址：_____

邮编：_____电话：_____传真：_____

磋商响应方全称（加盖公章）：

法定代表人（签字或盖私章）：

日期：

附件十二：

初次报价一览表

采购项目名称：　　采购编号：

序号	内容	磋商报价
1	**首届联合国世界地理信息大会官网安全防护项目**	小写：_____元 大写：_____元

注：报价表上的价格**应包括服务款、专用工具、保险、税金、代理费等，招标范围内全部工作内容等一切费用，**其市场风险由磋商响应方承担。

磋商响应方全称：

法定代表人或授权代表（签字）：

日期：