ICS 35.110
L 09

CA

中国通信工业协会团体标准

T/CA701-2024

信息化建设企业
信息系统业务安全服务能力评定标准
（2024 版）

Information construction enterprises

Criteria for evaluation of Information system business security service capability

2024-3-10 发布　　2024-04-01 实施

中国通信工业协会　　发布

目　次

前　言

本标准按照GB/T 1.1—2020《标准化工作导则第1部分:标准化文件的结构和起草规则》的规则起草。

本标准由中国通信工业协会提出并归口。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本标准主要起草单位：中国通信工业协会信息安全分会、吉林省电子信息产品检验研究院、安徽省电子产品监督检验所、湖北省资质服务认证中心。

本标准主要起草人：林迅、王晨光、李巍巍、苏奇、陈瑾、梁胜、李炜玉、李照轩。

本标准发布之日起，代替T/CA701-2020。

引　言

为进一步保障国家信息化建设工作的安全推进，加强网络和信息系统安全服务的规范化管理，推动行业技术进步，促进信息化建设企业提升核心竞争力，特制订本标准。

本标准依据国家信息化建设的相关文件，结合国内信息化建设企业的发展现状，以及中国通信工业协会在通信及信息数据管理等方面的成功经验，对信息化建设企业的安全服务能力提出了要求，为从事信息系统建设、信息化产品研发和信息安全服务和工业自动化等各类型企业提供了管理指南和实施规范。

本标准以信息化建设企业的服务行业领域（横向）和信息安全服务能力水平（纵向）为基础，提出了信息系统业务安全服务能力双维度评定方法。通过评定，可以充分展现信息化建设企业的专业服务方向和安全服务水平，也为相关管理部门开展行业数据采集与分析、信息化建设需方选择信息化建设企业提供了评价依据。

本标准是由中国通信工业协会、吉林省电子信息产品检验研究院、安徽省电子产品监督检验所、湖北省资质服务认证中心及相关行业专家基于市场和行业发展需要而共同制订，有利于发挥行业自律和示范作用，有效促进信息化建设企业完善自身管理体系，提高产品质量和服务水平，实现行业健康、可持续发展。

信息化建设企业信息系统业务安全服务能力评定标准

1 范围

本标准规定了信息化建设企业的信息系统业务安全服务能力的评定要求、评定结果以及评审机构的要求。本标准适用于：

a）从事信息化建设、工业自动化的企业，需要建立第三方能力评定体系或自评体系时；

b）中国通信工业协会或第三方评审机构评定企业能力时；

c）信息化建设需方评估和选择供方时；

d）其他适用的场合。

2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅注日期的版本适用于本文件。凡是不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB/T 19001 质量管理体系 要求

GB/T 4754—2017 国民经济行业分类与代码

ISO 10006：1997 质量管理 项目管理质量指南

3 术语和定义

下列术语和定义适用于本标准。

3.1 信息系统 Information system

指由计算机硬件、网络和通信设备、计算机软件、信息资源、信息用户和规章制度等等所组成的以处理信息流为目的的人机一体化系统。

3.2 业务 Business

指信息化建设需方的业务领域。

3.3 安全 security

指信息系统信息化工程全生命周期内的安全，包括信息系统的设计、实施、升级优化、运行维护

及数据安全保障等全过程的安全。

3.4 信息系统业务安全服务 Information system business security service

指在信息系统信息化工程全生命周期内提供的包括保障信息系统建设和运营的咨询、设计、实施、升级优化、运行维护及数据安全保障等在内的所有服务行为的统称。

3.5 信息系统业务安全服务能力评定 Evaluation of Information system business security service capability

依据本标准，对信息化建设企业信息系统业务安全服务能力的符合性评价。

3.6 信息化建设企业 Information construction enterprises

指在中华人民共和国境内依法设立的，专注于为信息化建设需方提供高品质的产品和行业应用解决方案的信息技术企业。信息化建设企业主要从事信息化产品的研发、制造、销售以及提供相关的信息技术服务。

注：信息化产品包括计算机软件、计算机硬件、计算机外围设备、网站建设、网络监控、协同办公、通讯设备、数据存储及信息安全等产品。

信息技术服务包括信息技术咨询、信息技术运维、设计开发服务、测试服务、数据处理服务、集成实施服务、培训服务、信息系统增值服务等服务。

3.7 信息安全服务业务项目额 Amount of Information Security Service Projects

指按照核算规则的要求对已完成的信息化建设项目合同进行拆分，通过拆分重新核算出的信息安全服务额度。

4 概述

本标准是信息化建设企业在信息化项目建设中提供服务的一种能力标定，有助于信息化建设企业强化自身建设和提升服务能力，自愿申报。

本标准以横、纵两个维度分别对信息化建设企业的服务行业领域和信息安全服务能力水平做出划分，并进行综合评定：

a）横向：依据信息化建设需方的行业领域为标准，分为八个行业领域：政府、公共服务、金融、电信、军工、商业、能源、工业企业；

注：行业领域划分参考《国民经济行业分类与代码（GB/4754-2017）》中的行业分类归纳而成。具体划分参见《附录 A 信息系统业务安全服务项目行业领域分类目录》。

信息化建设企业在申报评定前，需明确申报的行业领域。

注：申报评定的行业领域是指**信息化建设需方**的行业领域。

例：若信息化建设需方为银行、证券机构、保险机构，则申报评定的行业领域为金融行业。

b）纵向：依据信息化建设企业的信息安全服务能力水平，分为四个级别，由低到高分别为四级（入门级）、三级（基础级）、二级（业务级）、一级（专家级）。

注：四级（入门级）——具有参与信息系统业务安全服务工作的能力，能够按照通用的服务要求开展信息化建设，提供基本的信息化产品和服务。

三级（基础级）——具有初级的信息系统业务安全服务能力水平。拥有相关技术储备，能够按照信息化建设需方的建设需求，提供基础性、通用性的信息化产品和服务。

二级（业务级）——具有较高的信息系统业务安全服务能力水平。了解申报行业领域的业务流程、业务特点，具备较强的研发能力或拥有自主研发的信息安全类产品。能够较好地把握信息化建设需方的建设需求，提供满足需求的信息化产品和解决方案。

一级（专家级）——具有极高的信息系统业务安全服务能力水平。熟悉申报行业领域的业务流程、业务特点并有深入研究，拥有大量的自主研发的信息安全类产品。能够准确地把握信息化建设需方的建设需求，提供优质的产品和解决方案，有助于信息化建设需方的信息化建设战略的落实和业务目标的实现。

5 评定原则

a）信息系统业务安全服务能力水平的等级评定应由低到高，逐级评定；

b）信息系统业务安全服务行业领域的评定可仅评定一个行业领域，亦可评定多个行业领域。

6 评定要求

信息系统业务安全服务能力评定是对申报企业的实力和行业领域的专业服务能力进行综合评价，包括综合条件、财务状况、业绩要求、管理能力、技术实力、人才保障六个方面。

6.1 一级要求

6.1.1 综合条件

a）企业是中华人民共和国境内注册的法人单位，且无不良信用记录；

b）企业取得信息系统业务安全服务二级资质的时间不少于两年；

c）企业拥有固定的办公场所，面积不少于一千平米；

d）企业依法经营，信誉良好；

e）企业有良好的履约能力。

6.1.2 财务状况

a）近两年度营业收入累计达到一亿元以上，财务数据真实可信，并经在中华人民共和国境内依法设立的会计师事务所审计；

b）企业财务状况良好，最近两年度没有出现亏损；

c）拥有与申报行业领域信息安全业务相适应的固定资产，固定资产净值至少一百万元。

6.1.3 技术实力

a）企业对申报行业领域的业务流程有深入研究，居国内同行业领先水平；

b）已建立完备的技术管理体系，并有效运行；

c）企业应建立产品、服务目录，并拥有与申报行业领域和新业务相适应的产品或服务解决方案；

d）企业在申报行业领域内，拥有经过登记的自主研发的信息安全类产品不少于十个，且在已完成的项目中得到了应用；

e）企业在技术研发方面持续投入，近年度技术研发费用占同期销售收入总额的比例不低于百分之五；

f）已建立产品开发与测试体系，具备独立的测试环境、必要的软、硬件设备及开发、测试工具。

6.1.4 业绩要求

a）近两年度在申报行业领域内完成的信息安全服务业务项目总额不少于五千万元。企业申报的项目应为自主研发的信息安全类产品项目，其中至少有一个以上项目且单个项目的信息安全服务业务项目额不少于五百万元或者至少有五个以上项目且单个项目的信息安全服务业务项目额不少于三百万元；

b）企业申报的项目均已通过验收并投入实际应用。

6.1.5 管理能力

a）依据ISO9001标准建立完备的质量管理体系，通过国家认可的第三方认证机构认证，证书在中国合格评定国家认可委员会（CNAS）工作网站上处于有效状态，且连续有效运行时间不少于一年；

b）依据ISO27001标准建立完备的信息安全管理体系，通过国家认可的第三方认证机构认证，且连续有效运行时间不少于一年；

c）依据项目管理知识体系标准（PMBOK）建立完备的项目管理体系，具备专业的项目管理工具，并有效运行；

d）已建立完备的信息安全服务项目知识库体系，并能在项目管理中有效应用；

e）已建立完备的客户服务管理体系和客户关系管理系统，并有效运行；

f）企业的主要技术负责人应具备相关专业硕士以上学位且从事信息安全服务业务技术工作不少于五年或者具备相关专业本科以上学历且从事信息安全服务业务技术工作不少于十年；

g）企业的财务负责人应具有会计专业技术高级资格。

6.1.6 人才保障

a）信息安全服务的工作人员应具备从事信息安全服务的知识、技能和经验；

b）从事信息安全服务的工作人员不少于一百人，占企业员工总人数的比例不低于百分之五十，其中从事技术研发的人数不少于二十人；

c）通过中国通信工业协会“信息系统业务安全服务工程师”能力培训的人数不少于二十人，且大学本科以上学历人员所占比例不低于百分之八十；

d）企业应识别信息安全服务工作人员的服务能力要求，明确信息安全服务工作人员的岗位职责和岗位技能要求，并确保信息安全服务工作人员能够胜任其承担的职责；

e）已建立完备的人力资源管理体系，并有效运行。

6.2 二级要求

6.2.1 综合条件

a）企业是中华人民共和国境内注册的法人单位，且无不良信用记录；

b）企业取得信息系统业务安全服务三级资质的时间不少于一年；

c）企业拥有固定的办公场所，面积不少于三百平米；

d）企业依法经营，信誉良好；

e）企业有良好的履约能力。

6.2.2 财务状况

a）近两年度营业收入累计达到五千万元以上，财务数据真实可信，并经在中华人民共和国境内依法设立的会计师事务所审计；

b）企业财务状况良好，最近年度没有出现亏损；

c）拥有与申报行业领域信息安全业务相适应的固定资产，固定资产净值至少五十万元。

6.2.3 技术实力

a）企业对申报行业领域的业务流程有深入研究，具有较高的技术水平；

b）已建立技术管理体系，并有效运行；

c）企业应建立产品、服务目录，并拥有与申报行业领域相适应的产品或服务解决方案；

d）企业在申报行业领域内，拥有经过登记的自主研发的信息安全类产品不少于五个，且在已完成的项目中得到了应用；

e）企业在技术研发方面持续投入，近年度技术研发费用占同期销售收入总额的比例不低于百分之五；

f）已建立产品开发与测试体系，具备独立的测试环境、必要的软、硬件设备及开发、测试工具。

6.2.4 业绩要求

a）近两年度在申报行业领域内完成的信息安全服务业务项目总额不少于两千万元。企业申报的项目应为自主研发的信息安全类产品项目，其中至少有一个以上项目且单个项目的信息安全服务业务项目额不少于三百万元或者至少有五个以上项目且单个项目的信息安全服务业务项目额不少于一百万元；

b）企业申报的项目均已通过验收并投入实际应用。

6.2.5 管理能力

a）依据ISO9001标准建立完备的质量管理体系，通过国家认可的第三方认证机构认证，证书在中国合格评定国家认可委员会（CNAS）工作网站上处于有效状态，且连续有效运行时间不少于一年；

b）依据项目管理知识体系标准（PMBOK）建立完备的项目管理体系，并有效运行；

c）已建立信息安全服务项目知识库体系，并能在项目管理中有效应用；

d）已建立完备的客户服务管理体系，并有效运行；

e）企业的主要技术负责人应具备相关专业硕士以上学位且从事信息安全服务业务技术工作不少于三年或者具备相关专业本科以上学历且从事信息安全服务业务技术工作不少于五年；

f）企业的财务负责人应至少具有会计专业技术中级资格。

6.2.6 人才保障

a）信息安全服务的工作人员应具备从事信息安全服务的知识、技能和经验；

b）从事信息安全服务的工作人员不少于五十人，占企业员工总人数的比例不低于百分之五十，其中从事技术研发的人数不少于十人；

c）通过中国通信工业协会“信息系统业务安全服务工程师”能力培训的人数不少于十人，且大学本科以上学历人员所占比例不低于百分之八十；

d）企业应识别信息安全服务工作人员的服务能力要求，明确信息安全服务工作人员的岗位职责和岗位技能要求，并确保信息安全服务工作人员能够胜任其承担的职责；

e）已建立完备的人力资源管理体系，并有效运行。

6.3 三级要求

6.3.1 综合条件

a）企业是中华人民共和国境内注册的法人单位，且无不良信用记录；

b）企业拥有固定的办公场所，面积不少于一百平米；

c）企业依法经营，信誉良好；

d）企业有良好的履约能力。

6.3.2 财务状况

a）近一年度营业收入累计达到一千万元以上，财务数据真实可信，并经在中华人民共和国境内依法设立的会计师事务所审计；

b）企业财务状况良好，最近年度没有出现亏损；

c）拥有与申报行业领域信息安全业务相适应的固定资产，固定资产净值至少十万元。

6.3.3 技术实力

a）企业具有较强的技术实力；

b）企业应建立技术管理制度并执行。

6.3.4 业绩要求

a）近一年度在申报行业领域内完成的信息安全服务业务项目总额不少于三百万元；

b）企业申报的项目均已通过验收并投入实际应用。

6.3.5 管理能力

a）依据ISO9001标准建立质量管理体系，通过国家认可的第三方认证机构认证，证书在中国合格评定国家认可委员会（CNAS）工作网站上处于有效状态，并有效运行；

b）企业须建立项目管理制度，并在项目中执行；

c）企业须建立客户服务管理制度并执行；

d）企业的主要技术负责人应具备相关专业本科以上学历且从事信息安全服务业务技术工作不少于一年；

e）企业的财务负责人应至少具有会计专业技术初级资格。

6.3.6 人才保障

a）信息安全服务的工作人员应具备从事信息安全服务的知识、技能和经验；

b）从事信息安全服务的工作人员不少于十人；

c）通过中国通信工业协会“信息系统业务安全服务工程师”能力培训的人数不少于五人；

d）企业应识别信息安全服务工作人员的服务能力要求，明确信息安全服务工作人员的岗位职责和岗位技能要求，并确保信息安全服务工作人员能够胜任其承担的职责；

e）企业须建立员工培训与绩效考核制度并有效执行。

6.4 四级要求

6.4.1 综合条件

a）企业是中华人民共和国境内注册的法人单位，且无不良信用记录；

b）企业拥有固定的办公场所；

c）企业依法经营，信誉良好；

d）企业有良好的履约能力。

6.4.2 财务状况

a）最近年度财务数据真实可信；

b）拥有与申报行业领域信息安全业务相适应的固定资产。

6.4.3 技术实力

a）企业具有一定的技术实力；

b）企业应建立技术管理制度并执行。

6.4.4 业绩要求

a）最近年度在申报行业领域内具有至少一个进行或完成的信息安全服务业务项目；

6.4.5 管理能力

a）依据ISO9001标准建立质量管理体系并有效运行；

b）企业须建立项目管理制度，并在项目中执行；

c）企业须建立客户服务管理制度并执行；

d）企业具有与申报领域相关的技术负责人，且从事信息安全服务业务技术工作不少于一年。

6.4.6 人才保障

a）企业有信息安全服务相关的工作人员，且应具备从事信息安全服务的知识、技能和经验；

b）通过中国通信工业协会“信息系统业务安全服务工程师”能力培训的人数不少于1人，或通过计算机技术与软件专业技术资格考试的“信息安全工程师”人数不少于1人。

c）企业应明确信息安全服务工作人员的岗位职责和岗位技能要求；

d）企业须建立员工培训与绩效考核制度并执行。

7 信息安全服务业务项目额核算规则

a）首先，按信息化建设合同是否包含集成服务类项目将合同划分为供货类合同和集成服务类合同；

b）其次，按产品类别的划分标准将合同所涉产品或服务进行分项拆分，计算出合同分项金额；

c）再次，用合同分项金额乘以核算比例计算出此分项的信息安全服务业务项目额；

d）最后，将全部分项的信息安全服务业务项目额相加，即得出此份合同的信息安全服务业务项目额。

注1：合同标的额不等于信息安全服务业务项目额。申报企业须提供满足评定条件要求所需的所有合同。

注2：信息安全服务业务项目额的核算详见《附录B 信息安全服务业务项目额核算表》。

8 评定结果

a）若申报企业完全符合本标准规定的评定条件，则评定结果为“通过”，颁发证书；

b）若申报企业存在不符合本标准规定的评定条件的情况，则评定结果为“不通过”；

c）评定结果每年复检一次、每三年复评一次。

9 评定结果的应用

a）可作为信息化建设企业信息系统业务安全服务能力的重要证明；

b）可作为政府相关部门进行事中、事后监管的重要参考；

c）可作为信息化建设需方选择信息化建设企业的一项重要依据；

d）其他相关用途的证明。

10 评审机构要求

信息系统业务安全服务能力的评审机构须通过中国通信工业协会相关部门的审核、培训并获得授权后，方可开展评审工作，具体要求如下：

a）是在中华人民共和国境内注册的企业法人或事业单位法人；

b）已按ISO/IEC 17020《各类检查机构运作的基本准则》或经认可的团体标准，建立质量管理体系，并能有效运行；

c）具备开展评审工作所需的办公、财务条件；

d）建立了规范化的评审流程；

e）配置有一定数量的专业评审人员；

f）认定授权所需的其他要求。

附 录 A

信息系统业务安全服务项目行业领域分类目录

序号	行业领域	客户界定
1	政府	政府及政府常设机构等
2	公共服务	交通运输、仓储和邮政业；水利、环境和公共设施管理业；居民服务、修理和其他服务业；教育；卫生和社会工作；公共管理、社会保障和社会组织；国际组织
3	金融	金融业
4	电信	信息传输、软件和信息技术服务业
5	军工	军队、航空、航天、船舶等
6	商业	批发和零售业；住宿和餐饮业；房地产业；租赁和商务服务业；科学研究和技术服务业；文化、体育和娱乐业
7	能源	电力、火力、风力、热力、燃气及水生产和供应业；农、林、牧、渔业；采矿业
8	工业企业	制造业；建筑业

行业领域划分：参考《国民经济行业分类与代码（GB/4754-2017）》中的行业分类归纳而成。

附 录 B

信息安全服务业务项目额核算表

信息安全服务业务项目额核算表（一级）

申报企业：　　合同编号：　　行业：

合同类别	产品类别				合同分项金额（万元）	核算比例（%）	核算金额（万元）	备注
供货类合同	硬件	第三方硬件	非安全类硬件	服务器类		3%		
				网络产品类		3%		
				客户端类		1%		
			安全类硬件	服务器类		6%		
				网络产品类		6%		
				客户端类		3%		
		自产硬件	非安全类硬件	服务器类		6%		须随该合同复印件一并提交该产品为公司自产的证明（如专利证书或著作权登记书等）
				网络产品类		6%		
				客户端类		3%		
			安全类硬件	服务器类		45%		
				网络产品类		45%		
				客户端类		25%		
	软件	第三方软件	非安全类软件			3%		
			安全类软件	服务器类		8%		

				网络类		8%		
				客户端类		3%		
		自产软件	非安全类软件			6%		须随该合同复印件一并提交该产品为公司自产的证明（如专利证书或著作权登记书等）
			安全类软件	服务器类		45%		
				网络类		45%		
				客户端类		25%		
集成服务类合同	硬件	第三方硬件	非安全类硬件	服务器类		4%		
				网络产品类		4%		
				客户端类		1%		
			安全类硬件	服务器类		18%		
				网络产品类		18%		
				客户端类		6%		
			服务费			8%		依据产品清单中安全产品所占比列核定
		自产硬件	非安全类硬件	服务器类		25%		须随该合同复印件一并提交该产品为公司自产的证明（如专利证书或著作权登记书等）
				网络产品类		25%		
				客户端类		6%		
			安全类硬件	服务器类		75%		
				网络产品类		75%		
				客户端类		65%		
			服务费			75%		依据产品清单中安全产品所占比列核定
	软件	第三方软件	非安全类软件			8%		
			安全类软件	服务器类		18%		
				网络类		18%		
				客户端类		6%		

			服务费			35%		依据产品清单中安全产品所占比列核定
		自产软件	非安全类软件			25%		须随该合同复印件一并提交该产品为公司自产的证明（如专利证书或著作权登记书等）
			安全类软件	服务器类		85%		
				网络类		85%		
				客户端类		75%		
			服务费			75%		依据产品清单中安全产品所占比列核定
软件开发或技术服务类合同		软件	服务费			100%		合计标的为100%软件开发或者技术服务
合计								

信息安全服务业务项目额核算表（二级）

申报企业：　　合同编号：　　行业：

合同类别	产品类别				合同分项金额（万元）	核算比例（%）	核算金额（万元）	备注
供货类合同	硬件	第三方硬件	非安全类硬件	服务器类		4%		
				网络产品类		4%		
				客户端类		1%		
			安全类硬件	服务器类		18%		
				网络产品类		18%		
				客户端类		6%		
		自产硬件	非安全类硬件	服务器类		22%		须随该合同复印件一并提交该产品为公司自产的证明（如专利证书或著作权登记书等）
				网络产品类		25%		
				客户端类		8%		

			安全类硬件	服务器类		60%		
				网络产品类		60%		
				客户端类		40%		
	软件	第三方软件	非安全类软件			3%		
			安全类软件	服务器类		18%		
				网络类		18%		
				客户端类		6%		
		自产软件	非安全类软件			22%		须随该合同复印件一并提交该产品为公司自产的证明（如专利证书或著作权登记书等）
			安全类软件	服务器类		60%		
				网络类		60%		
				客户端类		45%		
集成服务类合同	硬件	第三方硬件	非安全类硬件	服务器类		8%		
				网络产品类		8%		
				客户端类		4%		
			安全类硬件	服务器类		25%		
				网络产品类		25%		
				客户端类		10%		
			服务费			12%		依据产品清单中安全产品所占比列核定
		自产硬件	非安全类硬件	服务器类		30%		须随该合同复印件一并提交该产品为公司自产的证明（如专利证书或著作权登记书等）
				网络产品类		30%		
				客户端类		15%		
			安全类硬件	服务器类		75%		
				网络产品类		75%		
				客户端类		65%		

			服务费			75%		依据产品清单中安全产品所占比列核定
	软件	第三方软件	非安全类软件			15%		
			安全类软件	服务器类		25%		
				网络类		25%		
				客户端类		12%		
			服务费			35%		依据产品清单中安全产品所占比列核定
		自产软件	非安全类软件			30%		须随该合同复印件一并提交该产品为公司自产的证明（如专利证书或著作权登记书等）
			安全类软件	服务器类		85%		
				网络类		85%		
				客户端类		75%		
			服务费			75%		依据产品清单中安全产品所占比列核定
软件开发或技术服务类合同		软件	服务费			100%		合同标的为 100%软件开发或者技术服务
合计								

信息安全服务业务项目额的核算表（三级）

申报企业：　　合同编号：　　行业：

合同类别	产品类别			合同分项金额（万元）	核算比例（%）	核算金额（万元）	备注
供货类合同	硬件	第三方硬件	非安全类硬件		5%		
			安全类硬件		25%		
		自产硬件	非安全类硬件		30%		须随该合同复印件一并提交该产品为公司自产的证

			安全类硬件		75%		明（如专利证书或著作权登记书等）
	软件	第三方软件	非安全类软件		5%		
			安全类软件		25%		
		自产软件	非安全类软件		30%		须随该合同复印件一并提交该产品为公司自产的证明（如专利证书或著作权登记书等）
			安全类软件		75%		
集成服务类合同	硬件	第三方硬件	非安全类硬件		5%		
			安全类硬件		75%		
			服务费		20%		依据产品清单中安全产品所占比列核定
		自产硬件	非安全类硬件		10%		须随该合同复印件一并提交该产品为公司自产的证明（如专利证书或著作权登记书等）
			安全类硬件		90%		
			服务费		75%		依据产品清单中安全产品所占比列核定
	软件	第三方软件	非安全类软件		5%		
			安全类软件		80%		
			服务费		45%		依据产品清单中安全产品所占比列核定
		自产软件	非安全类软件		15%		须随该合同复印件一并提交该产品为公司自产的证明（如专利证书或著作权登记书等）
			安全类软件		90%		
			服务费		75%		依据产品清单中安全产品所占比列核定
软件开发或技术服务类合同	软件		服务费		100%		合同标的为100%软件开发或者技术服务
合计							

附 录 C

网络关键设备和网络安全专用产品目录

网络关键产品（参考）

序号	产品类别	范围
1	网络和终端 隔离产品	在不同的网络终端和网络安全域之间建立 安全控制点 ， 实现在不同的网络终端和网 络安全域之间提供访问可控服务的产品
2	网络安全审计产品	采集网络、信息系统及其组件的记录与活动数据,并对这些数据进行存储和分析,以实现事件追溯、发现安全违规或异常的产品
3	网络脆弱性扫描产品	利用扫描手段检测目标网络系统中可能存在的安全弱点的软件或软硬件组合的产品
4	虚拟专用网产品	在互联网链路等公共通信基础网络上建立专用安全传输通道的产品
5	防病毒网关	部署于网络和网络之间 ， 通过分析网络层 和应用层的通信 ， 根据预先定义的过滤规 则和防护策略实现对网络内病毒防护的产品
6	统一威胁管理产品	通过统一部署的安全策略 ， 融合多种安全功能 ,针对面向网络及应用系统的安全威胁进行综合防御的网关型设备或系统
7	安全网络存储	通过网络基于不同协议连接到服务器的专用存储设备
8	终端接入控制产品	提供对接入网络的终端进行访问控制功能的产品
9	虚拟专用网络产品（VPN）	提供加密和隧道技术，用于在公共网络上建立安全的远程访问连接
10	远程访问控制产品	用于控制和监控远程访问到网络和系统的权限和活动
11	网络安全审计工具	对网络和系统进行全面审计和检查，查找系统漏洞和安全风险
12	网络安全咨询和威胁情报	提供网络安全方面的咨询、风险评估和威胁情报服务，帮助组织指定有效的安全策略和应对方案
13	网络安全审计和合规性解决方案	帮助组织评估网络安全政策的合规性，并提供符合法规要求的安全控制和报告

客户端类产品（参考）

序号	产品类别	范围
1	路由器	整系统吞吐量(双向) ≥12Tbps 整系统路由表容量 ≥55万条
2	数据备份与恢复产品	能够对信息系统数据进行备份和恢复 ， 且 对备份与恢复过程进行管理的产品
3	反垃圾邮件产品	能够对垃圾邮件进行识别和处理的软件或软硬件组合,包括但不限于反垃圾邮件网关、反垃圾邮件系统、安装于邮件服务器的反垃圾邮件软件,以及与邮件服务器集成的反垃圾邮件产品等
4	网站数据恢复产品	能够对垃圾邮件进行识别和处理的软件或软硬件组合,包括但不限于反垃圾邮件网关、反垃圾邮件系统、安装于邮件服务器的反垃圾邮件软件,以及与邮件服务器集成的反垃圾邮件产品等 .
5	安全操作系统	从系统设计、实现到使用等各个阶段都遵循了一套完整的安全策略的操作系统,目的是在操作系统层面保障系统安全
6	公钥基础设施	支持公钥管理体制,提供鉴别、加密、完整性和不可否认服务的基础设施
7	网络安全态势感知产品	通过采集网络流量、资产信息、日志、漏洞信息、告警信息、威胁信息等数据,分析和处理网络行为及用户行为等因素,掌握网络安全状态,预测网络安全趋势,并进行展示和监测预警的产品
8	信息系统安全管理平台	对信息系统的安全策略以及执行该策略的安全计算环境、安全区域边界和安全通信网络等方面的安全机制实施统一管理的平台
9	网络型流量控制产品	对安全域的网络进行流量监测和带宽控制的流量管理系统
10	信息过滤产品	对文本、图片等网络信息进行筛选控制的产品
11	USB移动存储 介质管理系统	对移动存储设备采取身份认证、访问控制、审计机制等管理手段,实现移动存储设备与主机设备之间可信访问的产品
12	文件加密产品	用于防御攻击者窃取以文件等形式存储的数据、保障存储数据安全的产品
13	数据销毁软件产品	采用信息技术进行逻辑级底层数据清除,彻底销毁存储介质所承载数据的产品
14	运维安全管理产品	对信息系统重要资产维护过程实现单点登录、集中授权、集中管理和审计的产品
15	日志分析产品	采集信息系统中的日志数据,并进行集中存储和分析的安全产品
16	身份鉴别产品	要求用户提供以电子信息或生物信息为载体的身份鉴别信息,确认应用系统使用者身份的产品
17	终端安全监测产品	对终端进行安全性监测和控制,发现和阻止系统和网络资源非授权使用的产品
18	电子文档安全管理产品	通过制作安全电子文档或将电子文档转换为安全电子文档,对安全电子文档进行统一管理、监控和审计的产品

19	杀毒软件	检测、阻止和清除计算机病毒、恶意软件和其他恶意代码
20	恶意软件分析产品	用于分析和研究位置的恶意软件，以便及时发现和应对新型威胁
21	数据加密产品	用于对敏感数据进行加密保护，以防止数据被未经授权的人访问和泄露
22	安全信息和事件管理产品（SIEM）	通过收集、分析和报告来自各种安全设备和系统的安全事件信息，帮助及时发现和响应安全威胁
23	两步验证产品（2FA）	通过将密码与其他身份验证方法（如短信验证码、指纹识别等）结合使用，提高用户账户的安全性
24	网络流量分析产品	用于分析网络流量，检测异常行为和潜在威胁，并提供实时警报和报告。
25	安全培训和教育	为员工提供网络安全意识和知识培训，帮助他们识别和防范网络威胁
26	身份和访问管理（IAM）	用于管理用户身份验证、授权和访问权限的解决方案，保护网络和系统免受未经授权的访问
27	Web应用程序防火墙（WAF）	专门用于保护Web应用程序免受攻击和数据泄露
28	文件和数据备份解决方案	定期备份关键文件和数据，以防止数据丢失和不可挽回的损失
29	涉密信息系统检查取证产品	用于保密行政管理部门利用技术手段对保密违法案件中涉及的计算机技术方面的情况进行核实确认，并从原始数据中寻找与泄密和违规相关的证据信息

服务器类产品（参考）

序号	设备类别	范围
1	交换机	整系统吞吐量(双向)≥30Tbps，整系统包转发率≥10Gpps
2	服务器(机架式)	CPU数量≥8个，单CPU内核数≥14个，内存容量≥256GB
3	可编程逻辑控制器(PLC设备)	控制器指令执行时间≤0.08微秒
4	防火墙	对经过的数据流进行解析 ，并实现访问控 制及安全防护功能的产品
5	入侵检测系统(IDS)	以网络上的数据包作为数据源,监听所保护网络节点的所有数据包并进行分析,从而发现异常行为的产品
6	安全数据库系统	从系统设计、实现、使用和管理等各个阶段都遵循一套完整的系统安全策略的数据库系统,目的是在数据库层面保障数据安全

7	入侵防御系统(IPS)	以网桥或网关形式部署在网络通路上,通过分析网络流量发现具有入侵特征的网络行为,在其传入被保护网络前进行拦截的产品
8	DDoS防护	提供分布式拒绝服务攻击防护，防止大流量的攻击对网络造成瘫痪
9	病毒防治产品	用于检测发现或阻止恶意代码的传播以及对主机操作系统应用软件和用户文件的篡改、窃取和破坏等的产品
10	负载均衡产品	提供链路负载均衡、服务器负载均衡、网络流量优化和智能处理等功能的产品
11	抗拒绝服务攻击产品	用于识别和拦截拒绝服务攻击、保障系统可用性的产品
12	数据泄露防护产品	通过对安全域内部敏感信息输出的主要途径进行控制和审计,防止安全域内部敏感信息被非授权泄露的产品
13	安全配置检查产品	基于安全配置要求实现对资产的安全配置检测和合规性分析,生成安全配置建议和合规性报告的产品