国家标准《信息安全技术 零信任参考体系架构》（征求意见稿）编制说明

一、 工作简况

1.1 任务来源

根据国家标准化管理委员会 2022 年下达的国家标准制修订计划，国家标准《信息安全技术 零信任参考体系架构》由网神信息技术（北京）股份有限公司负责承办，计划号：20220157-T-469。该标准由全国信息安全标准化技术委员会归口管理。

1.2主要起草单位和工作组成员

主要起草单位：奇安信网神信息技术（北京）股份有限公司、中国信息通信研究院、中国科学院软件研究所、中国科学院大学、国家计算机网络应急技术处理协调中心、中国科学技术大学、飞天诚信科技股份有限公司、国家信息技术安全研究中心、中国科学院信息工程研究所、北京天融信网络安全技术有限公司、公安部第三研究所、北京数字认证股份有限公司、江苏易安联网络技术有限公司、国民认证科技（北京）有限公司、启明星辰信息技术集团股份有限公司、深圳竹云科技股份有限公司、格尔软件股份有限公司、海信集团控股股份有限公司、大唐高鸿信安（浙江）信息科技有限公司、北京奇虎科技有限公司、上海派拉软件股份有限公司、杭州安恒信息技术股份有限公司、上海观安信息技术股份有限公司、国网区块链科技（北京）有限公司、兴唐通信科技有限公司、厦门市美亚柏科信息股份有限公司、北京百度网讯科技有限公司、北京远鉴信息技术有限公司、国家工业信息安全发展研究中心、中国信息安全测评中心、国家信息中心、公安部第一研究所、成都卫士通信息产业股份有限公司、中能融合智慧科技有限公司、北京信安世纪科技股份有限公司、长春吉大正元信息技术股份有限公司、中国科学院数据与通信保护研究教育中心、中国移动通信集团公司、深圳市腾讯计算机系统有限公司、北京协和医院、新华三技术有限公司、北京芯盾时代科技有限公司、北京神州绿盟科技有限公司、杭州海康威视数字技术股份有限公司、华为技术有限公司、云从科技集团股份有限公司、深信服科技股份有限公司、北京安博通科技股份有限公司。

工作组成员：齐向东、吴云坤、张彬、刘勇、张泽洲、安锦程、荆继武、詹榜华、李新友、张立武、左晓栋、邬怡、韩永刚、孟楠、赵泰、张严、刘丽敏、郭莉、陈亮、朱鹏飞、陆舟、王哲麟、李海玲、姚叶鹏、韩冬旭、刘治平、王龑、陈妍、刘占斌、夏冰冰、秦益飞、杨正权、李俊、韩少波、蒋蓉生、王文路、戴立伟、郑强、高雪松、何晨迪、郑驰、梅宗林，张睿、茆正华、黄铭恺、谢江、杨珂、蔡子凡、许雪姣、程长高、朱红星、郑榕、孙岩、孙明亮、国强、黄卉、苏智睿、汪仕兵、周开宇、李海宁、焦靖伟、索瑞军、李敏、于乐、赵蓓、蔡东赟、孟晓阳、万晓兰、尹晓东、鲁曈、陈加栋、王雨晨、李军、訾然、种竹。

1.3主要工作过程

（1）2020 年 3 月至 2020 年 4 月，网神信息技术（北京）股份有限公司、中国科学院大学、中国信息通信研究院、国家计算机网络应急技术处理协调中心、北京国信京宁信息安全科技有限公司、飞天诚信科技股份有限公司、国民认证科技（北京）有限公司、北京信安世纪科技股份有限公司、兴唐通信科技有限公司、启明星辰信息技术集团股份有限公司、海信集团有限公司等单位组成标准编制组，正式提出国家标准立项申请，并开展零信任架构参考体系架构的标准编写工作，对 NIST（美国国家标准与技术研究院）特别出版物 SP800-207《零信任架构》开展研究，参考国外零信任架构的应用场景、体系架构和部署等，调研国内零信任的应用需求、体系架构、产品现状和应用方案，讨论并确定标准的范围、框架及主要技术内容，完成《信息安全技术 零信任架构 参考体系架构》（草案）。

（2）2020 年 5 月，信安标委 2020 年第一次工作组线上会议周，在 WG4 工作组全体会议上，向专家和工作组其他成员单位汇报了《信息安全技术 零信任架构 参考体系架构》（草案）工作情况，听取专家及工作组其他成员单位的意见，经 WG4 工作组全体成员单位投票，同意本标准立项申请并上报信安标委。信安标委 WG1 和工作组组长联席会议对立项建议进行审议，建议将标准名称由《信息安全技术 零信任架构 参考体系架构》更改为《信息安全技术 零信任参考体系架构》。

（3）2020 年 9 月 3 日，召开《信息安全技术 零信任参考体系架构》第一次编制组专家线上工作会议，对标准编制的组织形式及任务分工进行了初次安排。

（4）2020 年 10 月 20 日、10 月 22 日，分别组织了线上、线下《信息安全

技术 零信任参考体系架构》第二次编制组专家工作会议和项目启动会，54 家参编单位代表参与本次会议，进一步明确本标准编制的组织形式及任务分工。

（5）2020 年 10 月 27 日，参加 WG4 工作组专家审查会，会议对 2020 年正式立项的标准制定项目和研究项目进行材料和进度审查，专家组对本标准草案文本提出相关修改意见，并安排对沈昌祥院士提出的“零信任十问”进行解释、回复，会后编制组按照会议精神，组织落实。

（6）2020 年 11 月 26 日，召开《信息安全技术 零信任参考体系架构》第三次编制组专家线上工作会议，通报了本次 WG4 工作组专家审查会情况，组织参编单位专家对“零信任十问”进行研讨，与会参编单位专家代表提出多项意见、建议，编制组根据会议精神对标准文本进行修改完善，整理“零信任十问”相关研讨意见。

（7）2021 年 3 月 10 日，参加 2020 年网络安全国家标准执行情况阶段性检查专家评审会，编制组汇报了本项目阶段性成果、存在的问题，以及下一步推进计划，收到检查组和与会专家的宝贵意见及建议，会后针对专家指出的问题积极组织整改。

（8）2021 年 3 月 23 日，召开《信息安全技术 零信任参考体系架构》第四次编制组专家线上工作会议。会议通报了阶段性检查专家评审会情况，对专家提出的问题及反馈意见展开讨论，对标准文本的修订与编制进一步沟通，与会参编单位专家代表提出多项意见、建议，标准编制组根据会议的评审意见对标准文本进行修改完善。

（9）2021 年 4 月 26 日，参加 WG4 工作组国家标准专家审查会，编制组汇报了本项目阶段性成果、院士意见专项整改报告、以及下一步推进计划，收到检查组和与会专家的宝贵意见及建议，会后针对专家指出的问题组织整改。

（10）2021 年 6 月 30 日，参加 2020 年网络安全国家标准项目研制情况抽查专家评审会，编制组汇报了项目组织开展情况、推进过程中存在的问题和下一步工作计划，收到检查组和与会专家的宝贵意见及建议，会后针对专家指出的问题积极组织整改。

（11）2021 年 7 月 7 日，召开《信息安全技术 零信任参考体系架构》第五次编制组专家线上工作会议。会议对 4 月、6 月参会情况进行通报，对专家提出的问题及反馈意见展开讨论，征集专家参加零信任研究报告撰写，会后根据会议

精神对标准文本进行修改完善。

（12）2021 年 7 月 14 日，标准牵头单位邀请邀请中国信息通信研究院、国家计算机网络应急技术处理协调中心、国家信息技术安全研究中心、中国科学院软件研究所、中国科学院信息工程研究所等参编单位专家，在北京奇安信安全中心会议室召开零信任编制组内部封闭研讨会，重点研究零信任核心关键问题，同时对标准文本进行大幅度修改完善。

（13）2021 年 8 月 20 日，信安密字[2021] 90 号文件，指定中国科学院软件研究所张立武研究员作为责任专家。

（14）2021 年 8 月 26 日，WG4 工作组召开国家标准《信息安全技术 零信任参考体系架构》专家审查会，编制组汇报了零信任标准推进情况，以及零信任研究报告编制情况，收到检查组和与会专家的宝贵意见及建议，会后针对专家指出的问题组织整改。

（15）2021 年 9 月 7 日，WG4 工作组召开国家标准《信息安全技术 零信任参考体系架构》指导会，深入指导编制组对标准草案文本进行修改，并对标准文本提出多项意见、建议。会后，编制组在责任专家带领下，针对专家指出的问题组织整改。

（16）2021 年 9 月 13 日，信安标委针对美国联邦机构近日发布的《联邦零信任战略》、《零信任成熟度模型》等政策文件，组织召开专题研讨会，就“美零信任战略部署及我国零信任相关工作建议”展开讨论，在国家安全可信框架下，研究具有中国特色的零信任，沈昌祥院士、高林副局长参会并发表重要论述。

（17）2021 年 9 月 17 日，WG4 工作组召开国家标准《信息安全技术 零信任参考体系架构》专家审查会，编制组汇报了零信任标准项目推进情况，专家一致同意通过标准草案的评审，并建议标准编制单位根据本次会议的意见修改后形成征求意见稿，会后针对与会专家的宝贵意见及建议组织整改。

（18）2021 年 10 月 15 日，标准牵头单位邀请在京部分参编单位专家，召开零信任编制组内部封闭研讨会，对最近几次会议专家提出的宝贵意见、建议进行研讨，同时对标准文本进行大幅度修改完善。

（19）2021 年 11 月 2 日，WG4 工作组召开国家标准《信息安全技术 零信任参考体系架构》指导会，深入指导编制组对标准草案文本进行修改，并对标准文本提出多项意见、建议。会后，编制组在责任专家带领下，针对专家指出的问

题组织整改。

（20）2021 年 11 月 11 日，召开《信息安全技术 零信任参考体系架构》第六次编制组专家线上工作会议，针对专家提出的问题及反馈意见展开讨论，对标准文本的修订与编制进一步沟通，会后根据会议精神，对标准文本进行修改完善。

（21） 2021 年 11 月 16 日，在信安标委 2021 年第二次标准周 WG4 工作组会议上，向与会专家及工作组成员单位汇报《信息安全技术 零信任参考体系架构》标准编制工作情况，听取了专家及工作组成员单位的意见，经工作组单位投票表决，同意本标准进入征求意见稿阶段。会后根据专家意见对标准文本进行了修订，形成征求意见稿。

（22） 2021 年 12 月 23 日，参加 WG4 工作组征求意见稿初稿专家评审会，编制组汇报了《信息安全技术 零信任参考体系架构》标准项目推进情况，专家组进行审查、质询和讨论，一致同意该项标准通过评审，建议公开征求意见。

（23）2022 年 2 月 18 日，参加 5 项网络安全国家标准征求意见稿专家审查会，编制组汇报了《信息安全技术 零信任参考体系架构》标准项目推进情况，专家组进行审查、质询和讨论，一致同意通过对该项标准的审查，建议编制组根据本次会议意见修改后，发起公开征求意见。

二、 标准编制原则和确定主要内容的论据及解决的主要问题

2.1编制原则

本标准基于我国的实际情况，遵从我国有关法律、法规的规定。具体原则与要求如下：

（1）实用性原则

本标准立足于当前国内零信任系统的实际状况，针对当前零信任所存在的错误描述和夸大宣讲，充分调研学术界成果和产业界实践，明确零信任概念定义，提出零信任参考体系架构。从而可以为采用零信任体系架构的用户单位、建设单位、测评单位及管理部门，在规划、设计、开发、应用时提供参考，帮助指导、规范和评估采用零信任体系架构系统的合规性、正确性和有效性，在进行零信任迁移和零信任能力建设演进时提供支持。

（2）合规性原则

本标准严格遵守《中华人民共和国网络安全法》、《中华人民共和国数据安全

法》、《中华人民共和国计算机信息系统安全保护条例》等法律法规的要求，立足于当前国内信息系统安全的实际状况，与相关标准协调一致。特别是和现有网络安全等级保护体系、可信计算技术体系等相结合，针对国内零信任实践，提出零信任参考体系架构。

（3）创新性原则

本标准深入学习零信任多年理论研究成果、广泛了解市场上的实践经验，参考国外零信任体系架构的理论研究、标准化工作和技术实践，吸收其精华。结合我国国情，基于我国信息化应用场景的探索实践，创新性的开展中国零信任标准化研究。总结、归纳、凝炼零信任概念、原则、架构和工程实践，在零信任实践支撑技术日益成熟，零信任作用得到实践验证条件下，提炼满足我国安全需求和适配我国应用场景的零信任体系架构，制定出具有先进水平的标准。

2.2编制思路及依据

（一）编制背景

零信任作为数据安全保护的安全理念和策略，经过 10 来年发展，已形成广受认可的技术架构及能力模型，作为支撑数据安全的关键技术，得到业界认可，零信任的广泛应用有利于提升和加快数据安全保障工作，促进以数据为关键要素的数字经济发展，也有利于支撑以“数字化转型”为主题的国家十四五规划。

2019年9月27日，工业和信息化部公开征求对《关于促进网络安全产业发展的指导意见（征求意见稿）》的意见，其中包括“积极探索拟态防御、可信计算、零信任安全等网络安全新理念、新架构，推动网络安全理论和技术创新。”

2021年3月，北京市发布《北京市“十四五”时期智慧城市发展行动纲要》，在第五项主要任务“把握态势、及时响应，保障安全稳定”中提出“建立健全与智慧城市发展相匹配的数据安全治理体系，探索构建零信任框架下的数据访问安全机制。”

2021年7月12日，工业和信息化部官网发布《网络安全产业高质量发展三年行动计划（2021-2023年）（征求意见稿）》，在第二章重点任务-第5点发展创新安全技术中，提出“推动网络安全架构向内生、自适应发展，加快开展基于开发安全运营、主动免疫、零信任等框架的网络安全体系研发。加快发展动态边界

防护技术，鼓励企业深化微隔离、软件定义边界、安全访问服务边缘框架等技术产品应用。”

此外，工业和信息化部在2020年11月发布的“2020年网络安全技术应用试点示范项目名单”中，“基于安全大数据和零信任的工业互联网安全防护平台”、“基于5G‘零’信任安全专网的全球协同设计及智能制造安全管理平台”入选工业互联网安全项目，“基于零信任现代IAM技术的智慧城市安全管控平台”、“远程办公零信任平台”入选智慧城市安全项目，均作为新型信息基础设施安全类网络安全技术应用试点示范项目；“基于零信任技术SDP安全接入平台”、“基于零信任体系的网络安全边界防护系统”入选网络安全公共服务类网络安全技术应用试点示范项目。在2021年9月发布的“2021年大数据产业发展试点示范项目名单”中，“面向垂直行业的零信任大数据安全访问平台建设及应用”，“基于零信任的大数据安全保护体系”入选大数据安全保障方向试点示范项目。

2019年以来，我国相关部委、部分央企、大型集团企业开始对零信任架构开展研究，目前，零信任已在金融、运营商、互联网企业、大型制造业、教育、政府科研、企事业单位等各行各业落地实施。但是零信任及零信任架构仍面临认识不统一、概念混淆的问题，网神信息技术（北京）股份有限公司联合在零信任“产学研用测”各方面均有代表性的单位组建了编制组，发挥各自优势，联合开展标准编制。

（二）编制思路

1）通过对零信任学术界、技术界、产业界的多方调研，梳理零信任相关技术成果，包括密码技术、身份安全、数据安全、设备管理、安全态势、威胁情报等，梳理归纳与零信任相关安全技术要求，总结凝练，支撑构建零信任体系框架，研究探索零信任技术实质。

2）在本标准研制的过程中，持续对零信任在美国、加拿大、新加坡、英国等多个国家的零信任实践进行调研、分析，对各国发布的零信任相关报告、规划等政策引导性文件进行跟踪，分析研究零信任在各国落地实践的技术路线、解决问题和应用效能，思考符合我国国情的零信任技术发展思路。

3）在标准研制过程，持续跟踪、调研国内外发布的，与零信任相关的各级各类标准，重点研究美国国家标准与技术研究院的 NIST.SP.800-207《零信任架构》，同步跟踪国内发布的零信任行业标准和团体标准，包括 GA/DSJ 351-2019

《公安大数据安全零信任体系技术设计要求》（内部发布）、T/CESA 1165-2021《零信任系统技术规范》、SCIE 005-2021《智慧城市零信任技术规范》、以及在CCSA 立项的《零信任安全技术参考框架》（报批稿）等，保持零信任体系架构的先进性和兼容性。

4）本标准在“持续动态性”、“细粒度”等方面对于访问控制策略的实施予以增强。GB/T 18794.3《信息技术开放系统互连 开放系统安全框架 第 3 部分:访问控制框架》定义了一个提供访问控制的通用框架。此处术语“开放系统”包括诸如数据库、分布式应用、开放分布式处理和开放系统互连这样一些领域。“安全框架”涉及定义对系统和系统内的对象提供保护的方法，以及系统间的交互。符合零信任解决资源安全保护问题的通用应用场景。

（三）编制依据及参考内容

本标准借鉴 NIST SP 800-207《零信任架构》主要思想、概念模型，将主体作为发起者、资源作为目标，引用 GB/T 18794.3《信息技术开放系统互连 开放系统安全框架 第 3 部分:访问控制框架》定义的通用访问控制框架，以及 GB/T 25069《信息安全技术 术语》定义的访问控制相关术语，按国家标准 GB/T 1.1-2020 规定的标准格式予以编写。

在身份管理方面参考 GB/T 31504—2015 信息安全技术 鉴别与授权 数字身份信息服务框架规范，以及 ISO/IEC 24760-1:2011 Information technology — Security techniques — A framework for identity management — Part 1: Terminology and concepts、ISO/IEC 24760-2:2015 Information technology -- Security techniques -- A framework for identity management -- Part 2: Reference architecture and requirements、ISO/IEC 24760-3:2016 Information technology — Security techniques — A framework for identity management — Part 3: Practice；在安全基线设计和遵循方面参考 GB/T 25070-2019 《信息安全技术 网络安全等级保护安全设计技术要求》、GB/T 34990—2017 信息安全技术《信息系统安全管理平台技术要求和测试评价方法》；在个人信息保护方面参考 GB/T 35273：2020《 信息安全技术 个人信息安全规范》相关规定；在访问控制实施方面参考 GB/T 30281—2013《信息安全技术 鉴别与授权 可扩展访问控制标记语言》、GB/T 29242—2012《信息安全技术 鉴别与授权 安全断言标记语言》等。

2.3解决的主要问题

本标准主要解决以下问题：

（1）提出数字时代下资源保护的安全理念

在当前数字化转型、万物互联的背景下，企业的 IT 基础设施发生了巨大变化，传统的物理边界安全防护面临越来越多的问题。通过物理隔离方式作用于边界上网络安全设备，如防火墙、入侵检测系统、VPN 等划分出与外网分隔的“内部安全区”无法再应对安全风险的挑战，需要基于“网络可能或已经被攻陷、存在内部威胁”的假定进行安全防护能力的构建。

零信任是应对网络安全新形势，更好的保护数字化时代的应用和数据资源的一种安全策略和理念，零信任架构把安全能力从边界，扩展到主体、行为、客体资源，构建“主体身份可信、业务访问动态合规、客体资源安全防护、信任持续评估”的动态综合纵深安全防御能力，降低资源访问过程安全的不确定性。

（2）明确零信任概念，澄清多种零信任错误说法

零信任起源于工程实践，相关厂商在“市场先行”营销策略下，零信任在初始传播过程出现了某些错误描述和夸大宣讲，如“零信任就是永不信任、什么都不信任”、“零信任是去边界、无边界”、“零信任是颠覆性的安全体系、新一代安全体系”，“零信任将替代 VPN、替代防火墙”等。偏离零信任本源，对零信任的发展带来不利影响。

通过标准制定，明确零信任概念，有助于统一认识，正本清源，正确引导零信任安全规划、建设实施。零信任一种以资源保护为核心的网络安全理念。认为对资源的访问，无论主体来自内部还是外部，主体和资源之间的信任关系都需要从零开始，通过持续环境感知与动态信任评估进行构建，从而实施访问控制。

（3）明确零信任体系架构组成

在零信任早期概念发展过程中，参与各方的技术思路、出发点有所不同，对于零信任的关注点也不一致，零信任概念呈现“百花齐放”的态势，但零信任的实质目标只有一个，就是以资源保护为核心，所有技术手段都是围绕这一目标共同开展零信任能力建设，不存在彼此之间的优劣对比。零信任架构是遵守最小权限原则，采用多属性动态访问策略，实现主体对资源的点对点访问控制。零信任体系架构既需要核心组件，也需要在支撑组件，共同实现零信任目标。

2.4主要内容

基于上述分析，本标准提出一套零信任参考体系架构，主要内容有 8 个章节：

第一章阐述本标准的目的及适用范围。

第二章列举制订本标准规范性引用的文件。

第三章对本标准中术语、定义进行规定，包括零信任、零信任体系架构等。

第四章对本标准中缩略语进行规定。

第五章介绍了零信任访问模型，以及基本组成。

第六章提出零信任体整体框架，描述主体、资源、核心组件、支撑组件。

第七章介绍了组件间的关系，包括主体与核心组件、支撑组件的关系，资源与核心组件、支撑组件的关系，支撑组件与核心主件的关系。

第八章介绍零信任体系架构工作流程，重点描述主体访问资源和动态调整访问策略的流程。

三、 主要试验[或验证]情况分析

暂无。

四、 知识产权情况说明

在本标准的前言中，声明了“请注意本标准的某些内容可能涉及专利。本文件的发布机构不承担识别这些专利的责任。”在标准制定期间，也恳请反馈意见单位“在提交反馈意见时，请将您知道的相关专利连同支持性文件一并附上”。截止目前，没有收到任何单位反馈的专利声明。

五、 产业化情况、推广应用论证和预期达到的经济效果

经历了十数年的研究和演化，零信任在理论、实验验证和实践积累了丰厚的沉淀。同时，云计算、大数据和人工智能等技术的发展也为零信任的实现提供了技术储备。近年来，党中央、国务院关于加强网络信息安全作出一系列重大决策部署，社会各界高度关注零信任创新发展，国家一直在引导探索零信任。国家部委、部分央企、大型集团企业等开始将零信任架构作为新建IT基础设施安全架构；银行、能源、通信等众多领域和行业也针对新型业务场景，开展采用零信任架构的关键技术研究和试点示范。在数字化发展、“新基建”和疫情防控等多因素牵引下，零信任目前已在金融、运营商、互联网企业、大型制造业、教育、政府科研、企事业单位等各行各业落地实施。从事零信任产品研发、解决方案、咨询调

研、教育培训和测评服务的安全厂商已近百余家。根据IDC和“安全牛”发布的研究报告，未来近八成的政府、公共事业、金融服务、互联网、能源、制造、交通运输、电信运营和教育等领域的用户有零信任规划或需求，市场规模有望在三年内突破百亿元。

本标准将明确零信任相关概念，提出零信任体系架构，为采用零信任体系架构的用户单位、建设单位、测评单位及管理部门，在规划、设计、开发、应用时提供参考，帮助指导、规范和评估采用零信任体系架构系统的合规性、正确性和有效性。同时，本标准在国家标准层面上对接身份鉴别、身份管理、风险评估、可信计算等相关信息安全标准，协同零信任相关方共同开展零信任动态综合纵深安全防御能力建设和演进，减少重复开发和部署，节省人力物力的投入，提升我国的信息安全自主化能力，对构建可控、有序、健康发展的网络生态具有重要战略意义和重大的社会价值。

六、 采用国际标准和国外先进标准情况

本标准属于自主制定标准，参考借鉴美国国家标准与技术研究院 NIST 特别出版物 SP800-207《零信任架构》定义的零信任体系架构，未采用其他国际标准和国外先进标准。

七、 与现行相关法律、法规、规章及相关标准的协调性

零信任架构标准与现行法律、法规、强制性国家标准及相关标准协调一致。

（一）严格遵循国家有关法规

本标准严格遵守《中华人民共和国网络安全法》、《中华人民共和国个人信息保护法》、《中华人民共和国数据安全法》、标准中所涉及身份管理、访问控制、鉴权认证、网络安全监控、风险评估等服务时，不得收集与提供的服务无关的数据及用户信息，依照法律、行政法规的规定和与用户的约定收集、使用、处理其保存的数据及个人信息。

标准中涉及的密码算法遵循《中华人民共和国密码法》、以及国家商用密码的有关规定等国家相关法律法规的规定。

（二）与相关国内相关标准的关系

零信任架构体系架构遵循《信息安全技术网络安全等级保护基本要求》、《信息安全技术网络安全等级保护测评要求》、《信息安全技术网络安全等级保护安全

设计技术要求》，作为关键网络安全产品参照标准，支持实现相关标准部分内容，同时自身安全性受相关标准约束。

八、 重大分歧意见的处理经过和依据

（一）零信任认识及相关论述分歧

2020 年 11 月，沈昌祥院士对零信任及相关论述进行思考，提出了相关意见和建议，汇总为《零信任十问》。标准编制组收到沈院士提出的意见后，在牵头单位总经理带领下，向沈院士汇报了零信任历史发展和标准制定工作开展情况，聆听了院士对于零信任标准整改的指示。多次组织全体参编单位专家召开研讨会，认真学习领悟沈院士意见及建议，思考零信任技术理念的基础性、前提性问题，梳理标准文本中零信任体系架构中相关描述，以及与已有信息安全国家标准衔接等问题，统一认识如下：

1） 零信任是一种以资源保护为核心的网络安全理念。需要对其信任情况进行持续评估，进而实施访问控制。零信任不是不信任，而是以已有的信任为基础，在对已有信任进行评估基础上，建立信任关系。例如采用可信密码模块（TCM）主机的信任等级会比未采用 TCM 模块的主机高。

2） 信任评估由零信任的策略引擎基于信任算法进行计算，计算信任的属性很多。包括人员属性、设备属性、行为偏差、业务遵从性等等。比如，对启用了可信计算基的设备，其信任等级高，未启用可信计算基的设备，其信任等级低。另外，执行信任评估的组件和信任评估所依赖的数据等，其自身的可信需要通过可信计算基进行保护。

3） 零信任只是一种安全策略和理念，在具体场景实施零信任策略时，需要一些技术组件，这些组件的相互关系形成一定的工程架构，零信任不涉及计算机体系结构的改变。零信任组件也需要采用现有安全技术手段进行防护，包括主机安全、网络安全、应用安全等技术都可用于对零信任组件进行保护。另外，零信任组件所在的计算环境和关键数据需要基于可信计算基确保其可信。

4） 物理网络边界永远存在，也需要边界安全防护，零信任是纵深防御的组成部分，是在边界安全基础之上进一步加强对资源的安全防护。

5） 零信任并未对访问控制机理进行改变，只是在“持续动态性”方面对于访问控制策略的实施予以增强。零信任的动态策略是通过策略判定点和实施点进

行的，零信任核心组件不涉及到代理，在一些特定业务场景，比如在远程访问场景，零信任的策略执行点可以和网络流量代理/网关进行集成。

6） 零信任实践中，资源机密性、完整性和可用性仍然是最基本的安全目标。“核心资产隐藏”不是零信任的核心理念。

7） 基于零信任的工程实践必须遵循等级保护相关要求。零信任体系架构与安全可信管理中心支持下的三重主动防护保护框架融合使用，共同发挥作用。三重防护框架为零信任提供信任基础和信任评估的数据源，零信任也可为可信管理中心提供更多维度的属性输入，比如行为基线偏离、业务违规风险、身份滥用风险等等。

8） VPN 所使用基于密码的连接协议等技术在零信任中仍然适用，并且零信任无论内外网，所有流量都必须加密，流量加密需要使用现有加密技术和协议进行。但对于一些远程接入场景，VPN 的接入只是一次性的身份验证，缺乏持续的验证和评估，这种情况，需要基于零信任的持续评估验证进行增强。

2021 年 9 月，信安标委组织召开零信任专题研讨会，就“美零信任战略部署及我国零信任相关工作建议”展开讨论，倡议在国家安全可信框架下，研究具有中国特色的零信任，沈院士参会并发表重要论述。

（二）零信任概念、原则及框架分歧

在零信任标准项目推进中，对于零信任的认识差距比较大，目前除了美国国家标准与技术研究院 NIST 特别出版物 SP 800-207《零信任架构》定义的零信任体系架构以外，没有其他学术界认可的统一认识，NIST SP 800-207 为英文撰写，行文习惯与标准表达存在差距，参编专家对英文解读、理解也不一致，围绕零信任概念、原则及框架产生很大分歧。

WG4 工作组对标准编制组开展多次专项指导帮助，围绕零信任核心本质问题，召开研讨会，反复讨论、多次调整零信任访问模型、基本原则、零信任支撑组件组成、定位等问题的描述，达成初步共识。

九、 标准性质的建议

建议本标准作为推荐性国家标准发布实施。

十、 贯彻标准的要求和措施建议

我国首部与数据安全相关的法律《数据安全法》也已于 9 月 1 日正式实施，

零信任作为数据安全保护的安全理念和策略，经过 10 来年发展，已形成广受认可的技术架构及能力模型，有利于支撑以“数字化转型”为主题的国家十四五规划，是国家数字经济发展的需要。零信任可满足多种数字化场景下，业务和数据的动态细粒度防护需求，在大型头部客户应用中，其技术成熟度已充分验证，在保护数据和应用方面，取得了很好的效果。比如，某部委基于零信任实施数据和业务访问的细粒度控制，大幅度降低对敏感数据的违规查询；某央企随着数字化转型深入，业务系统集中上云，基于零信任进行互联网出口收缩，增强整体防护水平；某大型银行大规模开展移动业务，基于零信任支撑移动办公常态化，实现业务支撑、降本增效和安全闭环。

在数字化发展、“新基建”和疫情防控等多因素牵引下，零信任产业迅速发展，零信任市场参与者越来越多，对于零信任的概念存在某些错误描述和夸大宣讲，对零信任体系架构也缺乏统一认识。本标准针对当前零信任及零信任架构认识不统一、概念混淆的问题，明确零信任定义、提出零信任参考体系架构，包括构建零信任体系架构的零信任访问模型、整体框架、组件及组件之间的关系，适用于为采用零信任体系架构的用户单位、建设单位、测评单位及管理部门，在规划、设计、开发、应用时提供参考，规范和评估其合规性、正确性和有效性。

本标准提出的零信任架构围绕数字化转型的需求背景，聚焦应用、服务、数据的保护，对于数字经济发展，很有意义。社会各界高度关注零信任创新发展，产业界和应用领域也亟待规范化的标准进行指导和协同，希望通过推出国家相关标准，尽快在概念、技术、产品、方案等层面形成标准化、规范化和体系化的指导。目前国内数据安全法、数据安全管理条例陆续出台，而零信任作为支撑大数据安全的关键技术之一，建议快速规范化落地。

十一、替代或废止现行相关标准的建议

无

十二、其它应予说明的事项

无

《信息安全技术 零信任参考体系架构》

标准起草组

二〇二二年二月