国家标准《信息安全技术 网络安全产品互联互通框架》

（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，《信息安全技术 网络安全产品互联互通框架》由北京赛西科技发展有限责任公司负责承办。该标准由全国信息安全标准化技术委员会归口管理，国标委计划号20230237-T-469。

1.2 制定背景

智能化、自动化的协同防护能力建设依赖于不同网络安全产品的互联互通。然而，当前我国网络安全产品互联互通仍在起步阶段。一方面，安全厂商产品类型复杂、不同产品的数据融合难、实现差异明显。大量研发成本用于实现不同安全厂商、安全产品之间的适配，同质化竞争严重，技术创新投入不足，创新能力有待提高，长期来看影响网络安全产业做大做强。另一方面，政务、电信、金融等行业用户单位通过研制数据、安全功能相关标准，研发定制化产品和安全管理平台等方式，初步实现在特定业务场景下的网络安全产品互联互通，但由于缺少统一技术框架和配套标准规范，用户单位网络安全产品互联互通工作改造成本高、效果不明显，难以形成规模化、可复制的应用推广经验。基于此，急需出台统一技术框架指导相关工作开展。

本文件拟提出统一的互联互通功能和互联互通信息框架，指导厂商、用户单位等开展网络安全产品互联互通建设工作，解决当前互联互通建设成本高，应用范围仅限于特定业务场景，难以复制推广的问题。

1.3 起草过程

（1）标准草案阶段

1） 2022 年 4 月至 6 月，组织国内主流安全厂商围绕国内外网络安全产品互联互通相关政策、标准规范、技术实现开展研究，形成标准草案第一稿。

2） 2022 年 7 月 1 日，编制组在北京组织召开了专家评审会，针对网络安全产品互联互通标准体系进行研讨，明确互联互通框架标准研制思路。

3） 2022 年 8 月 5 日，面向安全厂商下发网络安全产品互联互通情况调研问卷，从

厂商侧调研网络安全产品互联互通实际需求。

4） 2022 年 8 月 12 日，调研国家互联网应急中心、信工所等行业用户单位关于网络安全产品互联互通建设现状及需求。

5） 2022 年 8 月 28 日，组织国家信息中心、国家互联网应急中心、中国移动等行业用户单位对互联互通概念与框架内容进行研讨，根据与会专家意见形成标准草案第二稿。

6） 2022 年 10 月 12 日，组织专家对互联互通框架标准草案第二稿技术内容进行评审，编制组根据与会专家意见进一步明确互联互通功能与互联互通信息内容，完善了标准文本，形成标准草案第三稿。

7） 2022 年 11 月 18 日至 11 月 30 日，根据互联互通框架初步形成告警与资产信息描述技术方案，组织国家信息中心、天融信、深信服、安恒、绿盟、青藤、安天、东软等开展告警与资产信息描述试点验证，根据试点验证结果修改完善互联互通框架标准技术内容，提升标准条款可行性与合理性，形成标准草案第四稿。

8） 2022 年 12 月 7 日，WG5 工作组召开全体会议，会上汇报了《信息安全技术 网络安全产品互联互通框架》草案研制情况。根据会议决议，《信息安全技术 网络安全产品互联互通框架》标准形成征求意见稿。

（2）标准征求意见稿阶段

1） 2022 年 12 月至 2023 年 4 月，编制组对 WG5 工作组全体会议上收到的意见建议进行研讨，对标准文稿结构进行调整，形成征求意见稿第一版。

2） 2023 年 4 月 26 日，根据工作组安排汇报框架标准试点验证方案，会后根据专家组意见对试点验证方案内容进行修改完善。

3） 2023 年 4 月至 5 月，调整附录 B 互联互通功能使用的互联互通信息，同步调整互联互通功能、互联互通信息内容，形成征求意见稿第二版。

4） 2023 年 5 月 15 日，根据工作组安排，编制组就框架标准研制情况进行汇报，会后就评审会上收到的专家意见对征求意见稿内容进行修改完善，形成征求意见稿第三版。

5） 2023 年 5 月 30 日至 6 月 1 日，WG5 工作组召开 2023 年第一次全体会议，会上汇报了《信息安全技术 网络安全产品互联互通框架》征求意见稿研制情况，会

后就2023年第一次全会上收到的意见建议对标准文稿进行完善，形成征求意见稿第四版。

6） 2023年6月28日，秘书处组织召开《信息安全技术 网络安全产品互联互通框架》等3项网络安全国家标准专家审查会，会上编制组汇报了框架标准主要技术内容、意见处理情况，经专家审议建议编制工作组根据本次会议意见修改后发起公开征求意见。会后编制组就评审会上收到的专家意见对征求意见稿内容进行完善，形成征求意见稿第五版。

1.4 编制的主要成员单位

北京赛西科技发展有限责任公司负责起草，国家信息中心、国家互联网应急中心、中国电子技术标准化研究院、中国科学院信息工程研究所、中国移动通信集团、北京大学、联通数字科技有限公司、天翼安全科技有限公司、沈阳东软系统集成工程有限公司、杭州安恒信息技术股份有限公司、深信服科技股份有限公司、北京天融信网络安全技术有限公司、北京神州绿盟科技有限公司、北京升鑫网络科技有限公司、安天科技集团股份有限公司、广电计量检测集团股份有限公司、华为技术有限公司、奇安信科技集团股份有限公司等单位共同参与了该标准的起草工作。

二、标准编制原则、主要内容及其确定依据

2.1 标准编制原则

本文件的编制原则是：

（1）通用性

本文件拟提出统一的互联互通功能和互联互通信息框架，指导厂商、用户单位等开展网络安全产品互联互通建设工作，降低不同安全厂商、安全产品的适配成本。

（2）实用性

根据我国国情、实际应用环境和国家有关政策编制本文件，使其在指导用户单位与安全厂商互联互通建设过程中具有很强的实用性。

（3）可行性

在标准研制过程中，根据标准技术内容成熟度情况依托中国网络安全产业联盟推动相关单位开展试点验证工作，确保标准条款的可行性。

（4）一致性

符合国家相关法律法规与政策文件，并于现行标准规范协调一致。

2.2 主要内容及其确定依据

本文件制定的依据为：

a）标准格式按照GB/T 1.1—2020标准要求编写。

b）参考以下政策文件与国家标准和行业标准：

- GB/T 28458-2020《信息安全技术 网络安全漏洞标识与描述规范》
- GB/T 28517-2012《网络安全事件描述和交换格式》
- GB/T 36643-2018《信息安全技术 网络安全威胁信息格式规范》
- GB/T 37027-2018《信息安全技术 网络攻击定义及描述规范》

网络安全产品互联互通框架包括网络安全产品的互联互通功能和互联互通信息。

互联互通功能的功能类型主要分为4类，包括识别功能、防护功能、监测功能和处置功能。功能接口支撑各类功能实现，规范接口的通信协议、请求方式以及应满足的安全机制。

互联互通信息的信息类型主要分为6类，包括行为信息、告警信息、资产信息、脆弱性信息、威胁信息和事件信息。信息描述规范互联互通信息的信息内容和信息格式。

附录A给出了网络安全产品互联互通典型应用场景。附录B给出了互联互通功能使用的互联互通信息。

本章4.2节互联互通功能包括4.2.1功能类型和4.2.2功能接口。4.2.1功能类型给出了识别、防护、监测、处置四类互联互通功能的具体内容。4.2.2功能接口对互联互通功能接口内容提出具体要求。

本章4.3节互联互通信息包括4.3.1信息类型和4.3.2信息描述。4.3.1信息类型给出了行为信息、告警信息、资产信息、脆弱性信息、威胁信息和事件信息六类互联互通信息的具体内容。4.3.2信息描述对互联互通信息描述内容提出具体要求。

2.3 修订前后技术内容的对比[仅适用于国家标准修订项目]

本文件为制定项目，暂不适用。

三、试验验证的分析、综述报告，技术经济论证，预期的经济效益、社会效益和生态效益

3.1 试验验证的分析、综述报告

2022年11月，根据互联互通架，初步形成了告警与资产信息描述技术方案，组织国家信息中心、国家互联网应急中心、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、深信服科技股份有限公司、杭州安恒信息技术股份有限公司、绿盟科技集团股份有限公司、沈阳东软系统集成工程有限公司、安天科技集团股份有限公司、北京升鑫网络科技有限公司等共10家单位开展告警与资产信息描述试点验证。

根据各试点单位反馈，标准条款基本能够覆盖现有网络安全产品互联互通过程中应提供的数据，表明标准条款在实际业务场景中可落地可实施，按照互联互通框架开展的网络安全产品互联互通建设工作具有一定通用性、可行性与实用性。

3.2 技术经济论证

无。

3.3 预期的经济效益、社会效益和生态效益

目前，我国政务、电信、金融等行业用户单位及国内主流安全厂商均已开展网络安全产品互联互通实践工作，各行业各企业对于网络安全产品互联互通框架的需求明显。网络安全产品互联互通框架能够指导网络安全产品互联互通的设计、开发和应用，降低安全厂商、安全产品的之间的适配成本，降低用户单位互联互通工作改造成本，提升互联互通工作建设效果。

四、与国际、国外同类标准技术内容的对比情况，或者与测试的国外样品、样机的有关数据对比情况

目前国际上没有网络安全产品互联互通框架相关国际标准。

五、以国际标准为基础的起草情况，以及是否合规引用或者采用国际国外标准，并说明未采用国际标准的原因

本文件为自主制定，以我国建立跨部门、跨行业高效联动的网络安全防护能力相关要求为基础，能够为我国网络安全产品互联互通工作提供有效指导。

目前国际上没有网络安全产品互联互通框架相关国际标准。

六、与有关法律、行政法规及相关标准的关系

本文件与现行法律、法规、强制性国家标准及相关标准协调一致。本文件在同《中华人民共和国网络安全法》《关键信息基础设施安全保护条例》《“十四五”国家信息化规划》《国家网络安全事件应急预案》等相关法律法规和政策文件及现行国家标准GB/T 28458-2020《信息安全技术 网络安全漏洞标识与描述规范》、GB/T 28517-2012《网络安全事件描述和交换格式》、GB/T 36643-2018《信息安全技术 网络安全威胁信息格式规范》、GB/T 37027-2018《信息安全技术 网络攻击定义及描述规范》协调一致基础上，在研制过

程中引用了GB/T 20986-2023《信息安全技术 网络安全事件分类分级指南》、GB/T 25066-2020《信息安全技术 信息安全产品类别与代码》、GB/T 30279-2020《信息安全技术 网络安全漏洞分类分级指南》相关内容，针对网络安全产品互联互通应用提出具体要求。

七、重大分歧意见的处理经过和依据

无。

八、涉及专利的有关说明

无。

九、实施国家标准的要求，以及组织措施、技术措施、过渡期和实施日期的建议等措施建议

建议本文件作为推荐性国家标准发布实施。标准发布后，将在标准起草单位内率先开展应用，并通过标准宣贯、标准应用指南等方式，推进标准落地应用。同时，从标准发布到标准实施，建议过渡期设置为6个月。

十、其他应当说明的事项

无。

《信息安全技术 网络安全产品互联互通框架》编制工作组

2023 年 7 月 17 日