附件 3:

联盟技术规范《网络安全技术 病毒防治产品互联互通接口内容和格式》（征求意见稿）编制说明

一、工作简况

1．任务来源

根据中国网络安全产业联盟的技术规范制修订计划，联盟技术规范《网络安全技术 病毒防治产品互联互通接口内容和格式》由北京安天网络安全技术有限公司牵头编制，该规范由中国网络安全产业联盟归口管理。

2．编制的主要成员单位

本规范由北京安天网络安全技术有限公司主要负责编制，北京赛西科技发展有限责任公司、中国电子技术标准化研究院、国家信息中心、北京天融信网络安全技术有限公司、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、深信服科技股份有限公司、北京升鑫网络科技有限公司、启明星辰信息技术集团股份有限公司、北京山石网科信息技术有限公司、江苏省未来网络创新研究院等单位共同参与了该规范的起草工作。

3．主要工作过程

2024年5月，网络安全产品互联互通工作组围绕网络安全产品互联互通的典型应用场景，开展34类网络安全专用产品互联互通情况调研，确定病毒防治产品为首批网络安全专用产品互联互通测试对象之一，计划开展病毒防治产品互联互通接口内容和格式规范研制工作。

2024年6月至7月，编制组开展规范预研工作，充分考虑病毒防治产品互联互通场景和信息共享、安全功能协同需求，结合实际项目工程经验，编制形成规范草案第一版。

2024年8月上旬，召开编制组会议，对草案内容进行讨论，编制形成规范草案第二版。

2024年8月下旬，联盟组织网络安全企业开展本规范的试点验证工作。

2024年10月，联盟组织召开立项评审会，立项通过并形成22条专家意见。

2024年11月，编制组根据专家意见对技术规范草案进行修改，形成规范征求意见稿。

二、编制原则，和确定主要内容的论据及解决的主要问题

1．制定的基本原则

本规范的编制遵循以下原则：

1）通用性

本规范拟提出统一的病毒防治产品互联互通的信息共享接口和功能协同接口，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规范，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

在规范研制过程中，根据规范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，确保规范条款的可行性。

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．确定主要内容的依据

依据GB/T AAAAA.1-20XX《网络安全技术 网络安全产品互联互通 第1部分：框架》（报批稿）、GB/T AAAAA.3-20XX《网络安全技术 网络安全产品互联互通 第3部分：告警信息格式》（送审稿）、GB/T 37090-2018 《信息安全技术 病毒防治产品安全技术要求和测试评价方法》等国家标准，确定了病毒防治产品与安全管理系统互联互通的信息为告警信息，互联互通的功能包括恶意代码检测和恶意代码处理，并细化了其他告警信息内容格式和接收的功能接口内容和格式。

3．解决的主要问题

由于不同厂商研制的各类网络安全产品在安全设置策略、技术实现路线、专利等方面存在差异，缺乏统一的信息共享接口和功能协同接口规范，导致网络安全产品存在难以实现高效互联互通的问题。病毒防治产品作为网络安全防护体系中的重要一环，其效能的发挥不仅依赖于自身的检测与防护能力，也体现在能否与其他安全管理系统实现高效的信息共享与功能协同。因此，亟需制定本规范，根据现有病毒防治产品互联互通实际需求，提

出统一的互联互通信息共享接口和功能协同接口，解决当前病毒防治产品难以有效协调联动和协同防护的问题，实现对恶意程序的快速应对，最大化发挥病毒防治产品的协同效能。

三、主要试验[或验证]情况分析

2024年8月，联盟依托中国电子技术标准化研究院赛西实验室按照本规范对3款病毒防治产品开展标准验证和产品检测工作，测试内容包含11类恶意程序告警信息报送接口以及6个恶意程序联动处置功能接口，共计42个测试项，根据检测结果，规范条款可覆盖现有病毒防治产品互联互通过程中应提供的数据和接收的功能指令，表明本规范条款在厂商侧能够落地实施，切合病毒防治产品互联互通的应用场景，能够指导其设计、研发生产。

四、专利情况说明

无

五、产业化情况、推广应用论证和预期达到的经济效果

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。病毒防治产品互联互通接口内容和格式规范能够指导此类产品互联互通功能的设计、开发、应用和测试，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。

六、与现行相关法律、法规、规章的协调性

本规范与现行法律、法规、强制性国家标准及相关标准协调一致。

七、重大分歧意见的处理经过和依据

无

八、贯彻联盟技术规范的要求和措施建议

本规范主要用于指导病毒防治产品互联互通功能的设计、开发、应用和测试，建议计划开展网络安全产品互联互通建设的用户单位、安全厂商等依据本规范给出的病毒防治产品互联互通接口内容和格式开展产品互联互通工作。

九、其他应予以说明的事项

无

《网络安全技术 病毒防治产品互联互通接口内容和格式》编制工作组

2024-11-15