ICS 33.050
CCS M 30

团　体　标　准

T/TAF 132-2022

网络产品供应链安全要求　物流要求

Security requirements for network product supply chain—
Logistics requirements

2022-09-15 发布　　2022-09-15 实施

电信终端产业协会　发布

目　　次

前言 II
1　范围 1
2　规范性引用文件 1
3　术语和定义 1
4　缩略语 2
5　物流要求概述 2
6　网络产品供应链物流安全管理通用要求 5
6.1 风险管理 5
6.2 物流服务商管理 5
6.3 物流技术和标准 6
6.4 物流 IT 系统安全 6
6.5 物流基础设施安全和准入控制 6
7　网络产品物流安全要求 7
7.1 运输管理 7
7.2 清关 7
7.3 仓储管理 7
7.4 逆向 8
7.5 软件的传输和交付 8
7.6 个人信息保护 9
参考文献 10

前　言

本文件按照 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》的规定起草。

本文件是网络产品供应链安全要求系列标准之一，该系列标准结构如下：

——《网络产品供应链安全要求》

——《网络产品供应链安全要求　采购要求》

——《网络产品供应链安全要求　物流要求》

——《网络产品供应链安全要求　制造要求》

请注意本文件中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。

本文件由电信终端产业协会提出并归口。

本文件起草单位：中国信息通信研究院、华为技术有限公司、联想（北京）有限公司、中兴通讯股份有限公司、新华三技术有限公司、成都泰瑞通信设备检测有限公司、杭州迪普科技股份有限公司、浪潮电子信息产业股份有限公司、深圳市腾讯计算机系统有限公司。

本文件主要起草人：张治兵、薄菁、郭春颖、刘兵、薛勇波、陈鹏、李汝鑫、刘俊、刘微、吴翔宇、周继华、吴萍、童天予、万晓兰、仇俊杰、宋桂香、倪平。

网络产品供应链安全要求　物流要求

1　范围

本文件提出了网络产品在物流环节的安全管理、组织机构和人员、信息系统等不同等级的安全要求，包括原材料的接收、存储、转运、产品包装、交付、逆向等过程的安全要求。

本文件适用于网络产品的提供者对供应链物流过程进行安全管理，也可为网络产品的采购者和第三方机构对网络产品物流过程进行安全性评价时提供参考。

2　规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；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 40050—2021　网络关键设备安全通用要求

GB/T 36637—2018　信息安全技术　ICT 供应链安全风险管理指南

T/TAF 073—2020　网络产品供应链安全要求

ISO 31000:2018　风险管理-准则 (Risk management — Guidelines)

3　术语和定义

下列术语和定义适用于本文件。

3.1

网络　network

是指由计算机或者其他信息终端及相关设备组成的按照一定的规则和程序对信息进行收集、存储、传输、交换、处理的系统。

[来源：T/TAF 073—2020，3.1]

3.2

网络产品　network product

是指作为网络组成部分以及维持网络功能的设备、软件等。

[来源：T/TAF 073—2020，3.2]

3.3

供应链　supply chain

通过多个资源和过程联系在一起的一系列组织，根据由服务协议或其他采购协议建立连续的供应关系，每个组织充当一个需求方、提供方或双重角色。

[来源：T/TAF 073—2020，3.3]

3.4

供应商　supplier

与需求方签订协议以提供产品或服务的组织或个人，具体包括：

——信息系统、系统部件或软硬件产品的开发者或生产者；

——货架产品供应商；
——产品经销商；
——提供运维等服务的服务商；
——提供运输仓储等物流服务的服务商等。
[来源：T/TAF 073—2020，3.7，有修改]

3.5

采购 purchase

指需求方在一定的条件下从供应市场获取产品或服务作为组织资源，以保证需求方生产及经营活动正常开展的一项经营活动。

[来源：T/TAF 073—2020，3.8，有修改]

3.6

物流 logistics

物品从供应地向接收地的实体流动过程。根据实际需要，将运输、储存、装卸、搬运、包装、流通加工、清关、配送、信息处理等基本功能实施有机结合。

[来源：T/TAF 073—2020，3.9，有修改]

3.7

关键部件 critical component

存储软件、数据的介质以及具备数据处理能力的部件。如芯片、存储介质、可编程控制器件等。

[来源：T/TAF 073—2020，3.10]

3.8

逆向 reverse

产品从网络产品的提供者客户处直接或通过渠道返回到网络产品的提供者，以及从网络产品供货方/厂商仓库、维修点(包括其所属自有维修点和维修服务商)等向其下一处理环节回运，进行检测、维修、再利用或报废的过程。

4 缩略语

下列缩略语适用于本文件。

TAPA FSR：运输资产保护协会 设施安全要求（Transported Assets Protection Association Facility Security Requirements）

TAPA TSR：运输资产保护协会 货车运输安全要求（Transported Assets Protection Association Trucking Security Requirements）

5 物流要求概述

网络产品供应链物流领域通常涵盖原材料运输、收货和存储，厂内和厂间原材料和半成品的转运和调拨，成品的包装防护设计，成品和配套物料的包装、分拣和标识，在途管理，站点交付，逆向管理等环节。与传统供应链物流重点为防损防盗抢不同的是，网络产品供应链进一步关注产品在物流过程中的防植入、防篡改、防伪造，保证网络产品完整的交付到下一环节直到最终客户。物流要求管理框架见图1。

图 1　物流要求管理框架

由于网络产品供应链在不同产品业务场景下，其物流环节安全管理要求存在差异。本文件将物流安全要求分为三个等级，即一级、二级和三级，安全等级由低到高，安全要求逐级增强。一级提出了保障供应链物流安全管理的基本要求。二级在基本要求的基础上，提升了包括对异常事件的管理流程、制度等要求，以增强供应链物流环节安全保障。三级在二级要求的基础上增加了标准化、资质等要求，并通过增加使用自动化、智能化工具和技术要求，对供应链物流环节提供较强的安全保障。每一等级定义了网络产品供应链在满足相应等级要求的最小集合，满足该等级标识的所有项目才能标识为该级别。物流安全要求等级划分见表 1。安全要求条目中的“ALL”表示一级、二级和三级均具有该要求，“L2，L3”表示二级和三级具有该要求，“L3”表示三级具有该要求。

表 1　物流安全要求等级划分表

物流安全要求			一级	二级	三级
6 网络产品供应链物流安全管理通用要求	6.1 风险管理	(a)	✓	✓	✓
		(b)	✓	✓	✓
		(c)	✓	✓	✓
		(d)	✓	✓	✓
		(e)	—	—	✓
		(f)	—	✓	✓
		(g)	—	—	✓
	6.2 物流服务商管理	(a)	✓	✓	✓
		(b)	✓	✓	✓
		(c)	✓	✓	✓
		(d)	✓	✓	✓
		(e)	✓	✓	✓
		(f)	—	✓	✓
		(g)	—	✓	✓
		(h)	—	✓	✓
		(i)	—	✓	✓
		(j)	—	—	✓
		(k)	—	—	✓
	6.3 物流技术和标准	(a)	✓	✓	✓
		(b)	✓	✓	✓
		(c)	✓	✓	✓
	6.4 物流 IT 系统安全	(a)	✓	✓	✓

表 1　物流安全要求等级划分表（续）

物流安全要求				一级	二级	三级
6 网络产品供应链物流安全管理通用要求	6.4 物流 IT 系统安全		(b)	✓	✓	✓
			(c)	✓	✓	✓
			(d)	✓	✓	✓
			(e)	—	✓	✓
			(f)	—	✓	✓
			(g)	—	✓	✓
	6.5 物流基础设施安全和准入控制		(a)	✓	✓	✓
			(b)	✓	✓	✓
			(c)	✓	✓	✓
			(d)	✓	✓	✓
7 网络产品物流安全要求	7.1 运输管理	7.1.1		✓	✓	✓
		7.1.2		✓	✓	✓
		7.1.3		—	✓	✓
		7.1.4		✓	✓	✓
		7.1.5		✓	✓	✓
		7.1.6		—	✓	✓
		7.1.7		—	—	✓
	7.2 清关	7.2.1		✓	✓	✓
		7.2.2		✓	✓	✓
		7.2.3		✓	✓	✓
		7.2.4		—	—	✓
	7.3 仓储管理	7.3.1		✓	✓	✓
		7.3.2		—	✓	✓
		7.3.3		—	—	✓
		7.3.4		✓	✓	✓
		7.3.5		✓	✓	✓
		7.3.6		✓	✓	✓
		7.3.7		✓	✓	✓
		7.3.8		✓	✓	✓
		7.3.9		✓	✓	✓
	7.4 逆向	7.4.1		✓	✓	✓
		7.4.2		✓	✓	✓
		7.4.3		✓	✓	✓
		7.4.4		✓	✓	✓
		7.4.5		✓	✓	✓
		7.4.6		✓	✓	✓
		7.4.7		✓	✓	✓
	7.5 软件的传输和交付	7.5.1 软件的交付	(a)	✓	✓	✓
			(b)	✓	✓	✓
			(c)	✓	✓	✓
		7.5.2 软件授权的交付	(a)	✓	✓	✓
			(b)	✓	✓	✓
	7.6 个人数据保护	7.6.1		✓	✓	✓
		7.6.2		✓	✓	✓

表 1　物流安全要求等级划分表（续）

物流安全要求			一级	二级	三级
7 网络产品物流安全要求	7.6 个人数据保护	7.6.3	✓	✓	✓
		7.6.4	✓	✓	✓
注 1：“—”表示不具有该要求；“✓”表示具有该要求。 注 2：表中物流安全要求对应本文件第 6 章至第 7 章。					

6　网络产品供应链物流安全管理通用要求

6.1　风险管理

网络产品的提供者应：

a) (ALL)建立风险管理制度或流程，确定责任部门或人员，定期对网络产品供应链物流环节的风险进行评估；
b) (ALL)由主管领导对评估的结论进行确认，组织制定风险应对预案，并安排资源进行风险的消减；
c) (ALL)每年至少进行一次风险应对预案刷新；
d) (ALL)保护供应链物流风险管理计划不受未经授权的披露和修改；
e) (L3)对高风险流程或者场景每年至少进行一次处置演练；
f) (L2，L3)依据 GB/T 36637-2018、ISO 31000:2018 等标准并结合本组织的业务流程和场景进行网络产品供应链物流环节的风险的评估，重点关注：可能导致完整性和真实性受到破坏的环节，可能导致物流服务商服务中断的因素，可能影响物流业务正常运行的核心基础设施；
g) (L3)联合物流服务商进行网络产品供应链物流环节风险的评估，并制定协同消减风险措施。

6.2　物流服务商管理

网络产品的提供者应：

a) (ALL)对候选物流服务商进行背景调查，选择信誉良好、服务质量优且满足安全要求的物流服务商；
b) (ALL)明确网络产品在物流环节的网络安全和隐私保护要求，如产品的包装要求、装车规范、封条要求、物流过程可视可追踪要求、收货验货要求、追溯要求、不扣货、保护货物完整性、按指定线路运输、指定线路颗粒度等；
c) (ALL)通过书面形式（如合同，协议或谅解备忘录等）将物流环节的网络安全和隐私保护要求，传递给物流服务商；
d) (ALL)建立对供应商的考核机制，物流服务商的考核应在每个考核周期内至少进行一次，对网络安全和隐私保护考核不合格的供应商应采取罚款、减少份额直至取消市场份额的措施，对不愿签署安全和隐私条款的物流服务商采取减少或取消市场份额的措施；
e) (ALL)对仓库管理员作业过程进行记录，并保障仓储作业过程可追溯；
f) (L2，L3)对仓库管理员进行法律法规、安全意识培训和背景调查；
g) (L2，L3)有多家可靠物流服务商可供选用，规划多条安全的物流线路可供使用；
h) (L2，L3)在物流服务商发生扣货、恶意破坏货物完整性、篡改单据等恶性影响网络安全和隐私保护的事件时，立即中止合作；
i) (L2，L3)定期对物流服务商进行包括网络安全和隐私保护的现场检查；

j) (L3)建立对物流服务商承运的在途货物进行安全评估的制度，必要时对其承运的货物进行安全评估，留存记录，确定符合完整性和一致性要求后方可交付到下一环节；
k) (L3)对物流策略定期或不定期进行评估和更新。对物流策略的评估包括物流节点、路径的评估，对物流策略的更新包括优化物流路径、备份可靠资源（口岸、节点、运输方案等）、构建网状路由、物流服务商的替换、运输方式变化、物流节点调整、路径变更等。

6.3 物流技术和标准

网络产品的提供者应：

a) (ALL)设立专门部门或专人对物流环节的安全标准和工艺技术进行跟踪和研究；
b) (ALL)制定产品包装的安全基线，通过流程融入、可供应性设计（DFSC）和可制造性设计（DFM）实现在产品开发过程的落地，并通过适当的流程进行落地验证，如转产/试产流程；
c) (ALL)制定自身的原材料或成品的转运、运输、清关、仓储、流通履行、逆向等物流过程的安全防护标准和操作指导书。

6.4 物流 IT 系统安全

网络产品的提供者应：

a) (ALL)由业务需求部门和 IT 团队对物流 IT 系统的需求、技术方案、项目计划、项目交付进行安全评审和验收；
b) (ALL)开发物流 IT 系统时，应遵从 IT 安全标准、数据保护设计规范和质量红线，作业系统与办公系统需有相应的网络防护措施；
c) (ALL)指定专人负责物流 IT 系统的安全，有效防御外部渗透和攻击，支撑物流业务连续可靠的运作；
d) (ALL)IT 团队应建立问题跟踪闭环、线上事件管理、数据备份等机制，并进行定期的演练，保证物流 IT 系统的安全稳定运行；
e) (L2，L3)IT 团队应建立物流 IT 系统的运行保障机制，落实对工作电脑、服务器、自动化装备、IoT 设备等接入终端的安全防护能力和入网安全检测；
f) (L2，L3)IT 团队应对系统业务数据进行分级管理，保障业务数据安全；
g) (L2，L3)对物流 IT 系统的外部攻击事件及时通报、系统加固和阻断攻击源，消除或缓解事件影响。

6.5 物流基础设施安全和准入控制

物理安全是保护供应链中产品完整性的基本措施，物流基础设施应满足物理安全的相关要求，并对网络安全关键部件存放区域、仓库等进行重点防护。

a) (ALL)网络产品的提供者及物流服务商应制定内部的物理安全的要求对物流过程中与产品安全防护相关的基础设施进行管理；
b) (ALL)网络产品的提供者及物流服务商应采取措施重点对网络安全关键部件存放区域的物理设施进行管理（如设立区域责任人，定期巡查、检测、维护等），防止其被破坏，保证这些设施的正常运行；
c) (ALL)网络产品的提供者及物流服务商应对仓储区域的门禁、安保等进行有效管理，防止非授权进入、非授权接触产品，重点关注网络安全关键部件、自研软件、产品及关键文档的存放区域，如对网络安全关键部件存放区域设置专人管理；并建立物资、人员等的出入日志记录；

d) (ALL)网络产品的提供者应识别与物流环节强相关的 IT 系统，对相关权限应进行审核并定期清理（含外部人员/ 离职转岗人员等），明确用户权限设置策略及口令管理要求，避免客户信息和交付信息泄露，防止实物流通中产品被篡改、被植入。

7 网络产品物流安全要求

7.1 运输管理

7.1.1 (ALL)网络产品的提供者应对货物仓储及到发运目的地（电子制造服务厂商、原材料仓、客户等）的运输过程进行安全管理，防止货物被植入、篡改、替换、伪造、破损、灭失。

7.1.2 (ALL)网络产品的提供者应提前规划运输路线、停留节点。

7.1.3 (L2，L3)网络产品的提供者应定期组织审视路由、节点安全，对风险节点进行分级管理，并根据路由节点风险等级选用安全线路及可靠的签署了网络安全和隐私保护协议的物流服务商。

7.1.4 (ALL)网络产品的提供者应根据整车整柜货物价值安排运输计划，匹配不同等级的安保措施/运输工具。

7.1.5 (ALL)网络产品的提供者应对货物进行明确和唯一的标识，如条码、固件哈希等且这些标识可以与采购订单、供应商、供应商生产信息等进行关联，根据该标识需方可以快速准确的追溯货物来源。

7.1.6 (L2，L3)网络产品的提供者应基于物流安全风险的识别与评估结果，对在运输过程中货物的失而复得、路由偏离、风险节点超期停留等异常场景，建立异常事件处理机制，进行分层分级管理。

7.1.7 (L3)网络产品的提供者应落实运输工具检查和承运人资质复核等管理要求，应用定位系统、电子锁等在途追踪与报警技术设备对运输工具进行实时监控与管理，当发生路线偏离、异常停留/开门等问题时，及时预警，启动预案及时处理。

7.2 清关

7.2.1 (ALL)网络产品的提供者如遇当地海关、商检或其他政府执法机关查验，在允许的情况下应要求物流服务提供商（LSP）、清关代理等全程陪同查验。

7.2.2 (ALL)在海关允许情况下，开箱查验前，物流服务商、清关代理需要对货物进行拍照，检验完毕封箱后要对货物再次进行拍照；照片、海关查验证明和开箱查验的信息如集装箱号、装箱单号或箱号等需妥善保管以备查阅。如果发现包装损坏或者货物缺失等情况，应针对异常情况拍照，书面记录货物异常情况，立即向需求方报告。

7.2.3 (ALL)网络产品的提供者应对未在正常清关周期内及时完成货物清关，被无正常理由长期滞留或扣押，涉及到关键部件的货物，进行安全风险评估，留存记录，以确定实物的应用与处理方式。

7.2.4 (L3)网络产品的提供者应根据业务的实际情况开展经认证的经营者（AEO）等相关资质认证并获证，减少开箱查验的频率。

7.3 仓储管理

7.3.1 (ALL)网络产品的提供者应建立仓储安全标准，对管辖范围内的库区周界、仓库出入控制、装卸码头和库区内作业等进行有效管理。

7.3.2 (L2，L3)网络产品的提供者应对原材料存储仓库建立专门的安全要求。

7.3.3 (L3)网络产品的提供者对原材料存储仓库的安保设施配置和相关技术应用应建立标准化管理体系，如符合 TAPA FSR、TAPA TSR、ISO 28000 等标准。

7.3.4 (ALL)网络产品的提供者应对仓库管理人员、作业人员和安保人员进行背景调查；通过培训提高仓储管理人员、作业人员及安保人员的安全防范意识和应对安全事件的处理能力，防止非授权进入、非授权接触产品，保障作业过程可记录、可追溯。

7.3.5 (ALL)网络产品的提供者租赁外部仓库时，应对仓储商进行背景审查；并与对方签订安全协议，确保物料安全，避免物料被篡改、损坏、盗窃等；应定期或者不定期的对租赁仓库作业和安全情况进行稽查。

7.3.6 (ALL)网络产品的提供者应重点对关键部件和产品进行在库安全管理，确保在库作业过程可记录、可溯源，在落实定期盘点的基础上，增加此类物料的盘点抽查，保障实物在库安全。

7.3.7 (ALL)网络产品的提供者的区域分支机构或仓库原则上只允许开展基础仓储业务，禁止进行软件加载测试。特定情况需软件加载测试应经相关部门审批后才可进行，并应采取防植入、防篡改措施，保留可追溯的加载和测试记录。

7.3.8 (ALL)网络产品的提供者在装车发运前应复核货物与出库单的一致性，检查包装封签完整性（含二次包装），并对车辆及装载情况拍照留档（整体装载情况、车辆状况、车厢封签等），遵照物流服务商管理标准对本地派送进行有效管理，确保运输过程安全、异常可追溯。

7.3.9 (ALL)网络产品的提供者应在收货时做好收货地址、收货人身份等复核查验工作。交接人应做严格外观检查，包括核对车辆和封条的完整性、一致性并拍照留证，以及货物包装完整性及货物数量真实性，若有异常应采取拍照、录像或原物封存等一项或多项方式进行留证，对异常货物进行标识隔离并立即报告。

7.4 逆向

7.4.1 (ALL)网络产品的提供者应对允许退货的网络产品进行来源、包装、标识、条码等检查，防止伪造品和非退货物料混入。

7.4.2 (ALL)网络产品的提供者应在逆向流程中采取措施防止使用伪造部件，防止再利用产品被植入恶意软件，保障逆向返回物料中的客户数据安全，确保可追溯。

7.4.3 (ALL)网络产品的提供者应对原包装已被破坏的网络产品进行安全评估和测试，评估、测试合格的网络产品可进入再利用流程。

7.4.4 (ALL)网络产品的提供者的维修中心应对返回的物料进行真实性、完整性检查，包括物料的外观、条码、编码、数量等，确保这些物料没有被篡改、植入和替换。

7.4.5 (ALL)网络产品的提供者对返回维修的网络产品应保障用户的个人信息和数据安全。

7.4.6 (ALL)网络产品的提供者应对回收的网络产品进行数据清除，数据清除后方可再利用。

7.4.7 (ALL)需要在本地报废的网络产品应使用经认证合格的报废服务商，报废服务商按照合同约定的方式处置物料，并提供报废证明。

7.5 软件的传输和交付

7.5.1 软件的交付

网络产品的提供者应：

a) (ALL)通过官方渠道进行软件的交付，使用方应通过授权的账户下载最新版本的软件或适配的软件版本；

b) (ALL)对软件（自研或外购）设置数字签名、数字证书等完整性验证工具；

c) (ALL)对以介质交付的软件，来料时需进行数字证书、数字签名、杂凑值等完整性的验证。发货时采取专门的包装并使用一次性防拆封签，并记录封签信息。接收时应检查封签的完整性，核对封签信息，安装时需要进行数字证书、数字签名、杂凑值的验证，无异常方可使用。

7.5.2 软件授权的交付

网络产品的提供者应：

a) (ALL)确定软件授权生成的方案，按合同、订单生成对应的软件授权，确保软件授权的生成是与合同、订单配置要求一致，并保存下载、激活记录；

b) (ALL)对退货订单的软件使用许可（软件 License）进行回收并在系统中标识，防止其被用于伪造品。

7.6 个人信息保护

7.6.1 (ALL)网络产品的提供者应识别隐私保护法规相关要求，并根据法规评估所采集、使用的个人信息的合规要点。如涉及敏感个人信息（例如运输轨迹、闭路电视监控、身份证、驾照号等），应进行专项的隐私风险评估，留存评估报告。

7.6.2 (ALL)网络产品的提供者在开展业务收集个人信息时或之前，需告知个人信息主体（如司机）收集的个人信息类型、个人信息处理的目的、方式、数据主体的权利和保护个人信息的安全措施。

7.6.3 (ALL)网络产品的提供者对获取的个人信息的使用、留存等处理过程，应与告知信息主体的声明内容保持一致。如有偏离，应评估合理性并提前告知数据主体。获取的个人信息应进行权限管控，避免未授权人员获取。

7.6.4 (ALL)因业务所需，涉及将获取的客户/物流服务商联系人信息告知第三方的情况，应与第三方约定明确个人信息保密、不能滥用、到期删除等个人信息保护要求。

参 考 文 献

[1] GB/T 24420—2009 供应链风险管理

[2] GB/T 32921—2016 信息安全技术 信息技术产品供应方行为安全准则

[3] GB/T 36637—2018 信息安全技术 ICT供应链安全风险管理指南

[4] ISO 28001:2007 Security management systems for the supply chain—Best practices for implementing supply chain security, assessments and plans—Requirements and guidance

[5] ISO/IEC 27036-2-2014 Information technology—Security techniques—Information security for supplier relationships—Part2: Requirements

[6] ISO/IEC 27036-3-2013 Information technology—Security techniques—Information security for supplier relationships—Part3: Guidelines for information and communication technology supply chain security

[7] NIST SP800-161 Supply Chain Risk Management Practices for Federal Information Systems and Organizations

电信终端产业协会团体标准

网络产品供应链安全要求　物流要求

T/TAF 132—2022

*

电信终端产业协会印发
地址：北京市西城区新街口外大街 28 号
电话：82052809
电子版发行网址：www.taf.org.cn