ICS 33.050
CCS M 30

团　体　标　准

T/TAF 131—2022

网络产品供应链安全要求　采购要求

Security requirements for network product supply chain—
Purchase 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

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、王勇、高媛媛、薛勇波、陈鹏、李汝鑫、施辰琛、刘俊、甘露、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　采购要求

1　范围

本文件提出了网络产品在采购环节的安全管理、组织机构和人员、信息系统等不同等级的安全要求，包括产品认证和供应商管理的安全要求。

本文件适用于网络产品的提供者对供应链采购过程进行安全管理，也可为网络产品的采购者和第三方机构对网络产品采购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。

T/TAF 073—2020　网络产品供应链安全要求

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

需求方　acquirer

获得或采购产品或服务的利益相关者，也可简称需方。在本文件中指网络产品的提供者。

[来源：T/TAF 073—2020，3.6，有修改]

3.5

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。本文件中包括供应链中提供软件或含软件的硬件及相关服务的所有供应商，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等。

[来源：T/TAF 073—2020，3.7，有修改]

3.6

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。

注：获取的产品或服务以商业交换为基础，不包括可以公开获取的资源，如开源软件等。

[来源：T/TAF 073-2020，3.8，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]

4 缩略语

下列缩略语适用于本文件。

CVSS：通用漏洞评分系统（Common Vulnerability Scoring System）

RFP：需求建议书（Request For Proposal）

SLA：服务级别协议（Service Level Agreement）

5 采购要求概述

网络产品供应链安全要求中的采购要求包括供应商安全管理组织及流程要求、供应商引入管理要求、供应商日常管理要求。采购要求管理框架见图 1。

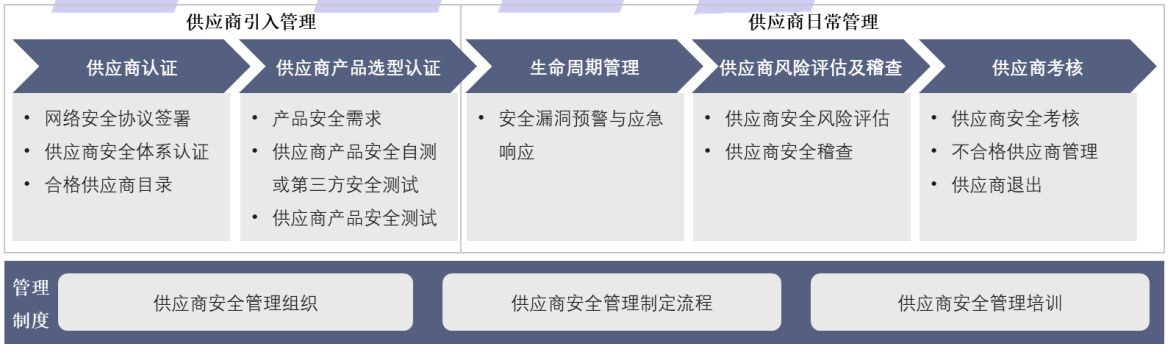

图 1 采购要求管理框架

由于网络产品供应链在不同产品业务场景下，其采购环节安全管理要求存在差异。本文件将采购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采购安全管理的基本要求。二级在基本要求的基础上，增加了可审计、可追溯要求，以增强供应链采购环节安全保障。三级在二级要求的基础上提升了管理流程、规范等要求，并通过增加使用自动化工具和技术要求，对供应链采购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。采购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　采购安全要求等级划分表

采购安全要求				一级	二级	三级
6 供应商安全管理组织及流程			(a)	✓	✓	✓
			(b)	✓	✓	✓
			(c)	✓	✓	✓
			(d)	✓	✓	✓
			(e)	✓	✓	✓
			(f)	✓	✓	✓
			(g)	✓	✓	✓
7 供应商引入管理	7.1 安全协议要求		(a)	✓	✓	✓
			(b)	✓	✓	✓
			(c)	✓	✓	✓
			(d)	✓	✓	✓
			(e)	✓	✓	✓
			(f)	—	✓	✓
	7.2 供应商安全体系要求		(a)	✓	✓	✓
			(b)	✓	✓	✓
			(c)	✓	✓	✓
			(d)	✓	✓	✓
			(e)	✓	✓	✓
			(f)	✓	✓	✓
			(g)	✓	✓	✓
			(h)	—	✓	✓
			(i)	—	✓	✓
			(j)	—	✓	✓
			(k)	✓	✓	✓
			(l)	—	—	✓
			(m)	—	—	✓
	7.3 供应商产品安全测试要求		(a)	✓	✓	✓
			(b)	—	✓	✓
	7.4 生产外包管理要求		(a)	✓	✓	✓
			(b)	✓	✓	✓
			(c)	✓	✓	✓
			(d)	—	✓	✓
			(e)	—	—	✓
8 供应商日常管理	8.1 供应商安全风险评估	8.1.1		✓	✓	✓
		8.1.2		✓	✓	✓

表 1　采购安全要求等级划分表（续）

采购安全要求				一级	二级	三级
8 供应商日常管理	8.1 供应商安全风险评估	8.1.3	(a)	✓	✓	✓
			(b)	✓	✓	✓
			(c)	✓	✓	✓
			(d)	✓	✓	✓
			(e)	✓	✓	✓
			(f)	✓	✓	✓
		8.1.4		✓	✓	✓
		8.1.5		✓	✓	✓
		8.1.6		—	✓	✓
	8.2 供应商安全漏洞预警与应急响应			✓	✓	✓
	8.3 供应商安全检查	8.3.1		✓	✓	✓
		8.3.2		✓	✓	✓
		8.3.3		✓	✓	✓
	8.4 供应商安全考核	8.4.1		✓	✓	✓
		8.4.2		✓	✓	✓
注 1：“—”表示不具有该要求；“✓”表示具有该要求。 注 2：表中采购安全要求对应本文件第 6 章至第 8 章。						

6　供应商安全管理组织及流程

需方应构建采购安全管理体系，以提高采购安全。采购安全管理体系应包含以下要求：

a) (ALL)建立供应商安全管理的组织，并定义供应商安全管理组织职责和要求；
b) (ALL)建立供应商安全管理的框架，明确供应商网络安全管理的目标及方法；
c) (ALL)建立供应商安全管理流程，包括供应商引入/认证、日常管理、退出等，并明确各阶段的供应商管理要求；
d) (ALL)建立并维护合格供应商目录，并根据供应情况及时更新目录内容；
e) (ALL)制定安全培训计划，将供应商安全管理培训纳入组织的培训计划中，并定期执行；
f) (ALL)分析采购的产品可能面临的安全风险（如产品被篡改、敏感信息泄露等），并制定相应的应对措施；
g) (ALL)建立采购业务连续性程序，定期分析采购的产品运维过程中可能面临的安全风险，并制定相应的应对措施。

7　供应商引入管理

7.1　安全协议要求

制定安全协议应符合T/TAF 073-2020 6.2.1 (a) 3)的要求。未签署安全协议的供应商，不宜进入合格供应商目录。

安全协议内容要求如下：

a) (ALL)采购涉及产品时，安全协议应包含产品安全相关要求，例如，供应商产品不得含有任何形式的木马、后门、蠕虫、病毒、恶意代码、未知功能及未知权限的要求，以及数据安全的要求等；
b) (ALL)采购涉及服务时，安全协议应包含服务安全相关要求，例如，服务过程中遵循当地相关法律法规相关要求，基于合同、书面协议等开展服务工作要求、服务过程中不得攻击客户网络、在客户网络植入后门要求，进入客户网络需要获得客户授权要求等；
c) (ALL)安全协议应包含体系安全相关要求，例如，供应商应建立安全保障体系，实施产品及/或服务的安全管理并定期进行安全自检，供应商应对关键安全岗位员工进行安全管理，供应商应在研发、生产制造（芯片烧录、软件加载、组装、测试等）、仓储、物流和采购等环节建立详细的安全过程记录，以确保过程的可追溯性等要求；
d) (ALL)安全协议应包含应急响应的相关要求，例如漏洞响应与修复 SLA 要求；
e) (ALL)安全协议应包含供应商违反安全协议时的处理方法，如违约赔偿、合同终止、减少份额等；
f) (L2，L3)安全协议应包含供应商安全审计要求。

7.2 供应商安全体系要求

供应商的认证或审核应符合T/TAF 073-2020 6.2.1 (a) 2)的要求。供应商认证和审核标准包含以下要求，供应商：

a) (ALL)应建立安全组织、政策、流程对产品进行全生命周期安全管理；
b) (ALL)应建立安全基线，对产品进行安全需求分析、威胁分析、安全架构设计、安全系统设计等；
c) (ALL)应建立安全测试规范，进行安全测试设计，并对产品进行安全测试，并对安全测试结果进行分析、评估，输出安全测试报告；
d) (ALL)应建立开源及第三方软件安全管理流程及规范，对使用的开源及第三方组件的选型、使用、维护进行管理，确保组件来源安全可靠，并通过正式渠道获取，且漏洞得到持续管控；
e) (ALL)应发布的软件及产品应基于安全的密码算法进行完整性保护，防止被篡改；
f) (ALL)应建立变更控制流程，对产品在需求方侧的变更进行控制；
g) (ALL)应具备有效的漏洞响应、披露和修复的机制及流程，并建立安全事件管理机制，在发现产品的安全问题时及时通知需方并提供解决方案；
h) (L2，L3)应建立开发过程中产品对内发布和变更流程，对自研、外包开发以及选用第三方的软件、硬件进行统一管理；
i) (L2，L3)应建立配置库，对开发/测试的过程文档、源码、开发测试工具、软件包、开源及第三方软件等进行受控管理；并且应对软件开发配置库进行安全管理，避免信息泄露等安全风险；
j) (L2，L3)应建立安全编码规范，明确安全编码和安全构建要求；
k) (ALL)应执行安全编码审计流程，识别编码安全问题，并给出消减计划；
l) (L3)应在软件版本发布前，进行恶意代码、漏洞扫描，对二进制文件与源代码的一致性进行验证，确保所有的二进制文件来源可靠；
m) (L3)应建立开源及第三方软件合规管理流程。

7.3 供应商产品安全测试要求

需方应制定供应商产品选型、测试流程，对供应商的产品进行安全核验，未通过安全核验的供应商产品不得进入合格供应商产品目录。

对供应商的产品安全测试应包括：

a) (ALL)需方应让供应商按照 RFP 中的安全需求进行测试并提供自行测试报告或第三方安全测试报告；
b) (L2，L3)需方对供应商交付的产品开展动态测试、恶意代码检测、漏洞检测、渗透测试等安全测试。

7.4 生产外包管理要求

需方应至少符合以下要求：
a) (ALL)评估外包可能引入的安全风险，并制定应对措施；
b) (ALL)对外包进行管理，明确允许或禁止外包的条件、外包方的选择、外包数据的管理等；
c) (ALL)与外包方签订的协议中，外包方的安全责任且不得低于组织内部相同或者类似部门的安全要求；
d) (L2，L3)对外包生产过程进行监控，至少包括外包过程中安全规范的落实情况，人员的安全意识等；
e) (L3)对多级外包制定明确的管理规范，明确允许或禁止的条件。

8 供应商日常管理

8.1 供应商安全风险评估

8.1.1 (ALL)制定供应商安全风险管理框架和安全风险管理计划，对供应商应在一个评估周期内至少执行一次安全风险评估，对发生安全事件的供应商应及时重新进行安全风险评估，安全风险评估应在一定时期内覆盖目录中所有的供应商。
8.1.2 (ALL)框架应定义风险容忍度，评估维度（过往历史、合同遵从、安全影响和成熟度）和评估方法及频率。
8.1.3 评估方法应包含以下安全要求：
a) (ALL)供应商安全组织、安全流程的建立及运行情况；
b) (ALL)供应商合同或协议中规定的安全要求的执行情况，是否存在违反合同或协议的情况；
c) (ALL)供应商是否出现安全事件及响应处置情况；
d) (ALL)供应商以往安全相关业绩，包括人员政策、程序和安全实践等；
e) (ALL)供应商主动管理安全的证据，例如持有或通过与产品或服务相关的安全认证；
f) (ALL)评估供应商产品供应中断、停止授权、拒绝提供产品升级或技术支持服务的风险，确保供应链弹性。
8.1.4 (ALL)安全风险评估完成后应对评估中发现的安全风险制定处置方案，实施安全风险处置计划，并持续监控风险，更新风险评估和处置策略。
8.1.5 (ALL)在供应商发生重大变化（如：供应商所在地发生影响正常供应的事件、供应商资本背景发生变更、供应商资质发生变化、供应商产品架构发生变化等），可能影响需方的供应链安全时，应重新对供应商进行安全评估。
8.1.6 (L2，L3)供应商应根据客户需求提供其自身供应链管理安全风险评估结果和改善措施，涉及到商业秘密的除外。

8.2 供应商安全漏洞预警与应急响应

(ALL)需方应建立供应商产品漏洞预警与应急响应流程，对供应商产品出现的漏洞进行处理，推动供应商按照合同或协议中的漏洞SLA要求采取行动，确保漏洞及时处置。

8.3 供应商安全检查

8.3.1 (ALL)应对供应商安全组织、政策的执行情况，产品的安全开发/测试、安全服务、应急响应、生产、仓储、物流以及安全人员管理等进行检查，以确保供应商遵守签订的合同、协议、SLA 或采购方规定的其它安全要求，保障供应连续性。

8.3.2 (ALL)根据组织特点、供应环境变化以及供应商日常安全表现、供应商安全风险评估结果等对供应商开展检查。

8.3.3 (ALL)检查中发现问题要予以记录、跟踪，并推动供应商进行整改。

8.4 供应商安全考核

8.4.1 (ALL)应将供应商的日常安全表现，包括安全组织、安全流程的建立及运作情况、安全事件、安全漏洞、应急响应、日常检查的结果等纳入考核。

8.4.2 (ALL)应对供应商在一个评估周期内进行一次安全考核，对于考核不合格的供应商应推动供应商进行整改，如果整改后还不合格的供应商应调整出合格供应商目录，对于考核严重不合格的供应商可直接调整出合格供应商目录。

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　采购要求

T/TAF 131—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