ICS 35.040
L 80

团 体 标 准

T/ISEAA XXX-2019

信息安全技术 网络安全等级保护大数据基本要求

Information security technology- Bigdata baseline for classified protection of cybersecurity

（征求意见稿）

20XX -XX-XX 发布　　20XX -XX-XX 实施

中关村信息安全测评联盟 发布

目　　次

目次 II
前言 IV
引言 V
信息安全技术 网络安全等级保护大数据基本要求 1
1 范围 1
2 规范性引用文件 1
3 术语和定义 1
4 概述 1
5 第一级安全要求 2
5.1 安全物理环境 2
5.2 安全通信网络 2
5.3 安全区域边界 3
5.4 安全计算环境 3
5.5 安全管理制度 3
5.6 安全管理机构 3
5.7 安全管理人员 4
5.8 安全建设管理 4
5.9 安全运维管理 5
6 第二级安全要求 5
6.1 安全物理环境 5
6.2 安全通信网络 6
6.3 安全区域边界 6
6.4 安全计算环境 6
6.5 安全管理中心 7
6.6 安全管理制度 8
6.7 安全管理机构 8
6.8 安全管理人员 8
6.9 安全建设管理 8
6.10 安全运维管理 9
7 第三级安全要求 11
7.1 安全物理环境 11
7.2 安全通信网络 11

7.3 安全区域边界 12
7.4 安全计算环境 12
7.5 安全管理中心 14
7.6 安全管理制度 14
7.7 安全管理机构 14
7.8 安全管理人员 15
7.9 安全建设管理 15
7.10 安全运维管理 16
8 第四级安全要求 17
8.1 安全物理环境 17
8.2 安全通信网络 18
8.3 安全区域边界 18
8.4 安全计算环境 18
8.5 安全管理中心 20
8.6 安全管理制度 21
8.7 安全管理机构 21
8.8 安全管理人员 21
8.9 安全建设管理 21
8.10 安全运维管理 23
9 第五级安全要求 24
附 录 A （规范性附录） 关于安全要求的选择和使用 24
参考文献 29

前　言

本标准按照GB/T 1.1—2009给出的规则起草。

本标准由中关村信息安全测评联盟提出并归口。

本标准起草单位：公安部第三研究所（公安部信息安全等级保护评估中心）、国家信息中心、杭州安信检测技术有限公司、新华三技术有限公司、华为技术有限公司、北京奇安信技术有限公司、腾讯云计算（北京）有限责任公司、阿里巴巴（北京）软件服务有限公司、中国移动通信集团有限公司

本标准主要起草人：

引　言

为了更好地适应国家大数据战略要求，满足大数据技术发展带来的安全防护诉求，提升数据安全保护的能力，增强数据安全管理力度，《信息安全技术 大数据安全保护基本要求》将GB/T 22239《信息安全技术 网络安全等级保护基本要求》的通用安全保护要求进行细化和扩展，提出网络运营者整体应实现的数据安全保护技术和管理要求。

本标准是网络安全等级保护相关系列标准之一。

与本标准相关的标准包括：

——GB/T 22240　信息安全技术　网络安全等级保护定级指南。

——T/ISEAA XXX 信息安全技术 大数据安全等级保护定级及测评工作指南

在本标准中，加黑部分表示较高等级中增加或增强的要求。

信息安全技术 网络安全等级保护大数据基本要求

1 范围

本标准规定了网络安全等级保护第一级到第四级大数据等级保护对象的安全保护要求，对第五级大数据等级保护对象的安全要求不在本标准中描述。

本标准适用于指导分等级的非涉密大数据等级保护对象的安全建设和监督管理。

注：第五级大数据等级保护对象是非常重要的监督管理对象，对其有特殊的管理模式和安全要求，所以不在本标准中进行描述。

2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅所注日期的版本适用于本文件。凡是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/T 22239-2019 信息安全技术 网络安全等级保护基本要求

GB/T 35274-2017 信息安全技术 大数据服务安全能力要求

GB/T 35295-2017 信息技术 大数据 术语

GB/T 35589-2017 信息技术 大数据 技术参考模型

3 术语和定义

GB/T 22239-2019、GB/T 35274-2017、GB/T 35295-2017界定的以及下列术语和定义适用于本文件。为了便于使用，以下重复列出了GB/T 35274-2017、GB/T 35295-2017中的某些术语和定义。

3.1

大数据 bigdata

具有数量巨大、来源多样、生成极快、且多变等特征并且难以用传统数据体系结构有效处理的包含大量数据集的数据。

[GB/T 35295-2017，定义2.1.1]

3.2

数据生命周期 data lifecycle

数据从产生，经过各种生存形态（包括数据采集、数据传输、数据存储、数据处理（如计算、分析、可视化等）、数据交换等），直至数据销毁的演变过程。

[GB/T 35274-2017，定义3.2]

4 概述

大数据的特征是体量大、种类多、聚合快、价值高，受到破坏、泄露或篡改会对国家安全、社会秩序或公共利益造成影响，大数据安全保护的原则以数据为核心，关注数据全生命周期包括数据采集、数据传输、数据存储、数据处理、数据交换和数据销毁等环节的安全。

根据GB/T 22240 信息安全技术 网络安全等级保护定级指南给出的定级对象基本特征和GB／T 35589-2017 信息技术 大数据 技术参考模型给出的大数据参考架构，大数据相关等级保护对象可抽象为大数据资源、大数据应用、大数据平台等三类组件，如图1所示。

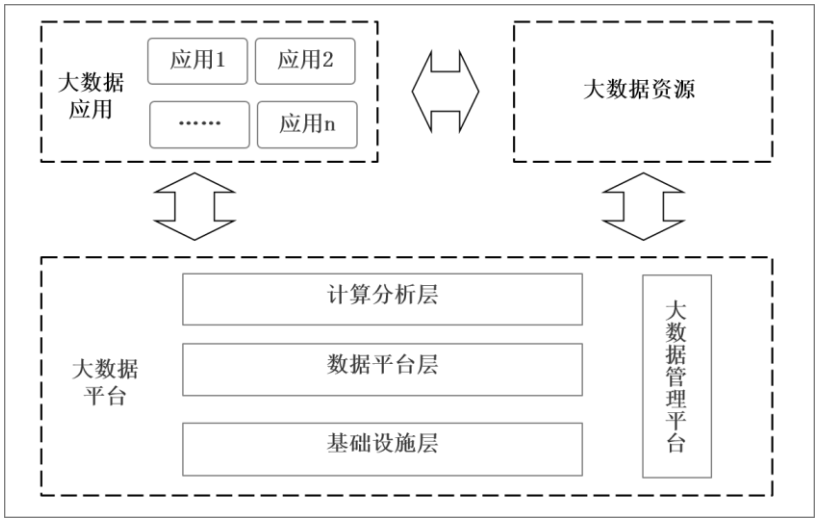

图1 大数据相关等级保护对象构成组件

大数据资源：具有数量巨大、来源多样、生成极快、且多变等特征并且难以用传统数据体系结构有效处理的包含大量数据集的数据。

大数据应用：基于大数据平台对数据执行处理过程，通常包括数据采集、数据传输、数据存储、数据处理、数据交换和数据销毁等环节。

大数据平台：为大数据应用提供资源和服务的支撑集成环境，包括基础设施层、数据平台层和计算分析层以及大数据管理平台等部分或者全部的功能。基础设施层提供物理或虚拟的计算、网络和存储能力；数据平台层提供结构化和非结构化数据的物理存储、逻辑存储能力；计算分析层提供处理大量、高速、多样和多变数据的分析计算能力，大数据管理平台提供大数据平台的辅助服务能力。大数据平台可以为多个大数据应用及大数据资源提供服务。

上述组件可能由不同运营者单独承担安全责任，从定级对象的责任主体角度出发，这些组件可独立或组合作为定级对象，例如大数据平台、大数据应用、大数据资源、大数据资源与大数据应用、大数据资源与大数据平台或大数据平台与大数据应用等，上述定级对象均可称为“大数据系统”。

5 第一级安全要求

5.1 安全物理环境

GB/T 22239-2019 6.1.1。

5.2 安全通信网络

5.2.1 网络架构

应保证大数据平台不承载高于其安全保护等级的大数据应用。

5.2.2 通信传输

GB/T 22239-2019 6.1.2.1。

5.2.3 可信验证

GB/T 22239-2019 6.1.2.2。

5.3 安全区域边界

GB/T 22239-2019 6.1.3。

5.4 安全计算环境

5.4.1 身份鉴别

GB/T 22239-2019 6.1.4.1。

5.4.2 访问控制

GB/T 22239-2019 6.1.4.2。

5.4.3 入侵防范

GB/T 22239-2019 6.1.4.3。

5.4.4 恶意代码防范

GB/T 22239-2019 6.1.4.4。

5.4.5 可信验证

GB/T 22239-2019 6.1.4.5。

5.4.6 数据完整性

本项要求包括：

a) GB/T 22239-2019 6.1.4.6；
b) 应采用技术手段对数据交换过程进行数据完整性检测；
c) 数据在存储过程中的完整性保护应满足数据源系统的安全保护要求。

5.4.7 数据保密性

应依据相关安全策略对数据进行静态脱敏和去标识化处理。

5.4.8 数据备份恢复

GB/T 22239-2019 6.1.4.7。

5.5 安全管理制度

GB/T 22239-2019 6.1.5。

5.6 安全管理机构

5.6.1 岗位设置

GB/T 22239-2019 6.1.6.1。

5.6.2 人员配备

GB/T 22239-2019 6.1.6.2。

5.6.3 授权和审批

本项要求包括：

a) GB/T 22239-2019 6.1.6.3；

b) 数据的采集应获得数据源管理者的授权，确保数据收集最小化原则。

5.7 安全管理人员

GB/T 22239-2019 6.1.7。

5.8 安全建设管理

5.8.1 定级和备案

GB/T 22239-2019 6.1.8.1。

5.8.2 安全方案设计

GB/T 22239-2019 6.1.8.2。

5.8.3 产品采购和使用

GB/T 22239-2019 6.1.8.3。

5.8.4 工程实施

GB/T 22239-2019 6.1.8.4。

5.8.5 测试验收

GB/T 22239-2019 6.1.8.5。

5.8.6 系统交付

GB/T 22239-2019 6.1.8.6。

5.8.7 服务供应商选择

GB/T 22239-2019 6.1.8.7。

5.8.8 大数据系统服务商选择

本项要求包括：

a) 应选择安全合规的大数据平台，其所提供的大数据平台服务应为其所承载的大数据应用提供相应等级的安全保护能力；

b) 应以书面方式约定大数据平台提供者的权限与责任、各项服务内容和具体技术指标等，尤其是安全服务内容。

5.8.9 供应链管理

应确保供应商的选择符合国家有关规定。

5.8.10 数据源管理

应通过合法正当渠道获取各类数据。

5.9 安全运维管理

GB/T 22239-2019 6.1.9。

6 第二级安全要求

6.1 安全物理环境

6.1.1 物理位置选择

GB/T 22239-2019 7.1.1.1。

6.1.2 物理访问控制

GB/T 22239-2019 7.1.1.2。

6.1.3 防盗窃和防破坏

GB/T 22239-2019 7.1.1.3。

6.1.4 防雷击

GB/T 22239-2019 7.1.1.4。

6.1.5 防火

GB/T 22239-2019 7.1.1.5。

6.1.6 防水和防潮

GB/T 22239-2019 7.1.1.6。

6.1.7 防静电

GB/T 22239-2019 7.1.1.7。

6.1.8 温湿度控制

GB/T 22239-2019 7.1.1.8。

6.1.9 电力供应

GB/T 22239-2019 7.1.1.9。

6.1.10 电磁防护

GB/T 22239-2019 7.1.1.10。

6.1.11 基础设施位置

应保证承载大数据存储、处理和分析的设备机房位于中国境内。

6.2 安全通信网络

6.2.1 网络架构

本项要求包括：

a) GB/T 22239-2019 7.1.2.1；

b) 应保证大数据平台不承载高于其安全保护等级的大数据应用。

6.2.2 通信传输

GB/T 22239-2019 7.1.2.2。

6.2.3 可信验证

GB/T 22239-2019 7.1.2.3。

6.3 安全区域边界

GB/T 22239-2019 7.1.3。

6.4 安全计算环境

6.4.1 身份鉴别

本项要求包括：

a) GB/T 22239-2019 7.1.4.1；

b) **大数据平台应能对不同客户的大数据应用进行身份鉴别；**

c) **大数据平台提供的重要外部调用接口应进行身份鉴别。**

6.4.2 访问控制

本项要求包括：

a) GB/T 22239-2019 7.1.4.2；

b) **对外提供服务的大数据平台，平台或第三方只有在大数据应用授权下才可以对大数据应用的数据资源进行访问、使用和管理；**

c) **应对数据进行分类管理；**

d) **应采取技术手段对数据采集终端、数据导入服务组件、数据导出终端、数据导出服务组件进行限制；**

e) **应最小化各类接口操作权限；**

f) **应最小化数据使用、分析、导出、共享、交换的数据集。**

6.4.3 安全审计

本项要求包括：

a) GB/T 22239-2019 7.1.4.3；

b) **大数据平台应对其提供的重要接口的调用情况进行审计；**

c) **应保证大数据平台服务商对服务客户数据的操作可被服务客户审计。**

6.4.4 入侵防范

GB/T 22239-2019 7.1.4.4。

6.4.5 恶意代码防范

GB/T 22239-2019 7.1.4.5。

6.4.6 可信验证

GB/T 22239-2019 7.1.4.6。

6.4.7 数据完整性

本项要求包括：

a) GB/T 22239-2019 7.1.4.7；
b) 应采用技术手段对数据交换过程进行数据完整性检测；
c) 数据在存储过程中的完整性保护应满足数据源系统的安全保护要求。

6.4.8 数据保密性

本项要求包括：

a) **大数据平台应提供静态脱敏和去标识化的工具或服务组件技术；**
b) 应依据相关安全策略对数据进行静态脱敏和去标识化处理；
c) **数据在存储过程中的保密性保护应满足数据源系统的安全保护要求。**

6.4.9 数据备份恢复

本项要求包括：

a) GB/T 22239-2019 7.1.4.8；
b) **备份数据应采取与原数据一致的安全保护措施。**

6.4.10 剩余信息保护

本项要求包括：

a) GB/T 22239-2019 7.1.4.9；
b) **数据整体迁移的过程中，应杜绝数据残留；**
c) 大数据平台应能够根据大数据应用提出的数据销毁要求和方式实施数据销毁。

6.4.11 个人信息保护

本项要求包括：

a) GB/T 22239-2019 7.1.4.10；
b) **采集、处理、使用、转让、共享、披露个人信息应在个人信息处理的授权同意范围内；**
c) **应采取措施防止在数据处理、使用、分析、导出、共享、交换等过程识别出个人身份信息。**

6.5 安全管理中心

6.5.1 系统管理

本项要求包括：

a) GB/T 22239-2019 7.1.5.1；
b) **大数据平台应为大数据应用提供管控其计算和存储资源使用状况的能力；**

c) **大数据平台应对其提供的辅助工具或服务组件，实施有效管理；**
d) **大数据平台应屏蔽计算、内存、存储资源故障，保障业务正常运行；**
e) **大数据平台在系统维护、在线扩容等情况下，应保证大数据应用的正常业务处理能力。**

6.5.2 审计管理

GB/T 22239-2019 7.1.5.2。

6.6 安全管理制度

GB/T 22239-2019 7.1.6。

6.7 安全管理机构

6.7.1 岗位设置

GB/T 22239-2019 7.1.7.1。

6.7.2 人员配备

GB/T 22239-2019 7.1.7.2。

6.7.3 授权和审批

本项要求包括：

a) GB/T 22239-2019 7.1.7.3；
b) 数据的采集应获得数据源管理者的授权，确保数据收集最小化原则。

6.7.4 沟通和合作

GB/T 22239-2019 7.1.7.4。

6.7.5 审核和检查

GB/T 22239-2019 7.1.7.5。

6.8 安全管理人员

GB/T 22239-2019 7.1.8。

6.9 安全建设管理

6.9.1 定级和备案

GB/T 22239-2019 7.1.9.1。

6.9.2 安全方案设计

GB/T 22239-2019 7.1.9.2。

6.9.3 产品采购和使用

GB/T 22239-2019 7.1.9.3。

6.9.4 自行软件开发

GB/T 22239-2019 7.1.9.4。

6.9.5 外包软件开发

GB/T 22239-2019 7.1.9.5。

6.9.6 工程实施

GB/T 22239-2019 7.1.9.6。

6.9.7 测试验收

GB/T 22239-2019 7.1.9.7。

6.9.8 系统交付

GB/T 22239-2019 7.1.9.8。

6.9.9 等级测评

GB/T 22239-2019 7.1.9.9。

6.9.10 服务供应商选择

GB/T 22239-2019 7.1.9.10。

6.9.11 大数据系统服务商选择

本项要求包括：

a) 应选择安全合规的大数据平台，其所提供的大数据平台服务应为其所承载的大数据应用提供相应等级的安全保护能力；
b) 应以书面方式约定大数据平台提供者的权限与责任、各项服务内容和具体技术指标等，尤其是安全服务内容。

6.9.12 供应链管理

应确保供应商的选择符合国家有关规定。

6.9.13 数据源管理

应通过合法正当渠道获取各类数据。

6.10 安全运维管理

6.10.1 环境管理

GB/T 22239-2019 7.1.10.1。

6.10.2 资产管理

本项要求包括：

a) GB/T 22239-2019 7.1.10.2；
a) **应建立数据资产安全管理策略，对数据全生命周期的操作规范、保护措施、管理人员职责等进行规定，包括并不限于数据采集、传输、存储、处理、交换、销毁等过程；**

b) 应对数据资产进行登记，建立数据资产清单。

6.10.3 介质管理

本项要求包括：

a) GB/T 22239-2019 7.1.10.3；

b) **应在中国境内对数据进行清除或销毁。**

6.10.4 设备维护管理

GB/T 22239-2019 7.1.10.4。

6.10.5 漏洞和风险管理

GB/T 22239-2019 7.1.10.5。

6.10.6 网络和系统安全管理

本项要求包括：

a) GB/T 22239-2019 7.1.10.6；

b) **应建立对外数据接口安全管理机制，所有的接口调用均应获得授权和批准。**

6.10.7 恶意代码防范管理

GB/T 22239-2019 7.1.10.7。

6.10.8 配置管理

GB/T 22239-2019 7.1.10.8。

6.10.9 密码管理

GB/T 22239-2019 7.1.10.9。

6.10.10 变更管理

GB/T 22239-2019 7.1.10.10。

6.10.11 备份与恢复管理

GB/T 22239-2019 7.1.10.11。

6.10.12 安全事件处置

GB/T 22239-2019 7.1.10.12。

6.10.13 应急预案管理

GB/T 22239-2019 7.1.10.13。

6.10.14 外包运维管理

GB/T 22239-2019 7.1.10.14。

7 第三级安全要求

7.1 安全物理环境

7.1.1 物理位置选择

GB/T 22239-2019 8.1.1.1。

7.1.2 物理访问控制

GB/T 22239-2019 8.1.1.2。

7.1.3 防盗窃和防破坏

GB/T 22239-2019 8.1.1.3。

7.1.4 防雷击

GB/T 22239-2019 8.1.1.4。

7.1.5 防火

GB/T 22239-2019 8.1.1.5。

7.1.6 防水和防潮

GB/T 22239-2019 8.1.1.6。

7.1.7 防静电

GB/T 22239-2019 8.1.1.7。

7.1.8 温湿度控制

GB/T 22239-2019 8.1.1.8。

7.1.9 电力供应

GB/T 22239-2019 8.1.1.9。

7.1.10 电磁防护

GB/T 22239-2019 8.1.1.10。

7.1.11 基础设施位置

应保证承载大数据存储、处理和分析的设备机房位于中国境内。

7.2 安全通信网络

7.2.1 网络架构

本项要求包括：

a) GB/T 22239-2019 8.1.2.1；

b) 应保证大数据平台不承载高于其安全保护等级的大数据应用；

c） **应保证大数据平台的管理流量与系统业务流量分离。**

7.2.2 通信传输

GB/T 22239-2019 8.1.2.2。

7.2.3 可信验证

GB/T 22239-2019 8.1.2.3。

7.3 安全区域边界

GB/T 22239-2019 8.1.3。

7.4 安全计算环境

7.4.1 身份鉴别

本项要求包括：

a） GB/T 22239-2019 8.1.4.1；

b） 大数据平台应能对不同客户的大数据应用进行身份鉴别；

c） **应对数据采集终端、数据导入服务组件、数据导出终端、数据导出服务组件的使用实施身份鉴别；**

d） **应对向大数据系统提供数据的外部实体进行身份鉴别；**

e） **大数据平台提供的各类外部调用接口应依据调用主体的操作权限进行相应强度的身份鉴别。**

7.4.2 访问控制

本项要求包括：

a） GB/T 22239-2019 8.1.4.2；

b） 对外提供服务的大数据平台，平台或第三方只有在大数据应用授权下才可以对大数据应用的数据资源进行访问、使用和管理；

c） **大数据平台应提供数据分类分级标识功能；**

d） **应在数据采集、传输、存储、处理、交换及销毁等各个环节，根据数据分类分级标识对数据进行不同处置，最高等级数据的相关保护措施不低于第三级安全要求，安全保护策略在各环节保持一致；**

e） **大数据平台应对其提供的各类接口的调用实施访问控制，包括但不限于数据采集、处理、使用、分析、导出、共享、交换等相关操作；**

f） 应最小化各类接口操作权限；

g） 应最小化数据使用、分析、导出、共享、交换的数据集；

h） **大数据平台应提供隔离不同客户应用数据资源的能力。**

7.4.3 安全审计

本项要求包括：

a） GB/T 22239-2019 8.1.4.3；

b） **大数据平台应保证不同客户大数据应用的审计数据隔离存放，并提供不同客户审计数据收集汇总和集中分析的能力；**

c） **大数据平台应对其提供的各类接口的调用情况进行审计；**

d) 应保证大数据平台服务商对服务客户数据的操作可被服务客户审计。

7.4.4 入侵防范

本项要求包括：

a) GB/T 22239-2019 8.1.4.4；

b) **应对导入或者其他数据采集方式收集到的数据进行检测，避免出现恶意数据输入。**

7.4.5 恶意代码防范

GB/T 22239-2019 8.1.4.5。

7.4.6 可信验证

GB/T 22239-2019 8.1.4.6。

7.4.7 数据完整性

本项要求包括：

a) GB/T 22239-2019 8.1.4.7；

b) 应采用技术手段对数据交换过程进行数据完整性检测；

c) 数据在存储过程中的完整性保护应满足数据源系统的安全保护要求。

7.4.8 数据保密性

本项要求包括：

a) GB/T 22239-2019 8.1.4.8；

b) 大数据平台应提供静态脱敏和去标识化的工具或服务组件技术；

c) 应依据相关安全策略和**数据分类分级标识**对数据进行静态脱敏和去标识化处理；

d) 数据在存储过程中的保密性保护应满足数据源系统的安全保护要求。

7.4.9 数据备份恢复

本项要求包括：

a) GB/T 22239-2019 8.1.4.9；

b) 备份数据应采取与原数据一致的安全保护措施；

c) **大数据平台应保证用户数据存在若干个可用的副本，各副本之间的内容应保持一致性；**

d) **应提供对关键溯源数据的备份。**

7.4.10 剩余信息保护

本项要求包括：

a) GB/T 22239-2019 8.1.4.10；

b) 数据整体迁移的过程中，应杜绝数据残留；

c) **大数据应用应基于数据分类分级保护策略，明确数据销毁要求和方式；**

d) 大数据平台应能够根据大数据应用提出的数据销毁要求和方式实施数据销毁。

7.4.11 个人信息保护

本项要求包括：

a) GB/T 22239-2019 8.1.4.11；

b) 采集、处理、使用、转让、共享、披露个人信息应在个人信息处理的授权同意范围内；
c) 应采取措施防止在数据处理、使用、分析、导出、共享、交换等过程识别出个人身份信息。

7.4.12 数据溯源

本项要求包括：
a) **应跟踪和记录数据采集、处理、分析和挖掘等过程，保证溯源数据能重现相应过程；**
b) **溯源数据应满足数据业务要求和合规审计要求。**

7.5 安全管理中心

7.5.1 系统管理

本项要求包括：
a) GB/T 22239-2019 8.1.5.1；
b) 大数据平台应为大数据应用提供管理其计算和存储资源使用状况的能力；
c) 大数据平台应对其提供的辅助工具或服务组件，实施有效管理；
d) 大数据平台应屏蔽计算、内存、存储资源故障，保障业务正常运行；
e) 大数据平台在系统维护、在线扩容等情况下，应保证大数据应用的正常业务处理能力。

7.5.2 审计管理

GB/T 22239-2019 8.1.5.2。

7.5.3 安全管理

GB/T 22239-2019 8.1.5.3。

7.5.4 集中管控

本项要求包括：
a) GB/T 22239-2019 8.1.5.4；
b) **应对大数据平台提供的各类接口的使用情况进行集中审计和监测。**

7.6 安全管理制度

GB/T 22239-2019 8.1.6。

7.7 安全管理机构

7.7.1 岗位设置

GB/T 22239-2019 8.1.7.1。

7.7.2 人员配备

GB/T 22239-2019 8.1.7.2。

7.7.3 授权和审批

本项要求包括：
a) GB/T 22239-2019 8.1.7.3；
b) 数据的采集应获得数据源管理者的授权，确保数据收集最小化原则；

c) **应建立数据集成、分析、交换、共享及公开的授权审批控制流程，依据流程实施相关控制并记录过程；**

d) **应建立跨境数据的评估、审批及监管控制流程，并依据流程实施相关控制并记录过程。**

7.7.4 沟通和合作

GB/T 22239-2019 8.1.7.4。

7.7.5 审核和检查

GB/T 22239-2019 8.1.7.5。

7.8 安全管理人员

GB/T 22239-2019 8.1.8。

7.9 安全建设管理

7.9.1 定级和备案

GB/T 22239-2019 8.1.9.1。

7.9.2 安全方案设计

GB/T 22239-2019 8.1.9.2。

7.9.3 产品采购和使用

GB/T 22239-2019 8.1.9.3。

7.9.4 自行软件开发

GB/T 22239-2019 8.1.9.4。

7.9.5 外包软件开发

GB/T 22239-2019 8.1.9.5。

7.9.6 工程实施

GB/T 22239-2019 8.1.9.6。

7.9.7 测试验收

GB/T 22239-2019 8.1.9.7。

7.9.8 系统交付

GB/T 22239-2019 8.1.9.8。

7.9.9 等级测评

GB/T 22239-2019 8.1.9.9。

7.9.10 服务供应商选择

GB/T 22239-2019 8.1.9.10。

7.9.11 大数据服务商选择

本项要求包括：

a) 应选择安全合规的大数据平台，其所提供的大数据平台服务应为其所承载的大数据应用提供相应等级的安全保护能力；
b) 应以书面方式约定大数据平台提供者的权限与责任、各项服务内容和具体技术指标等，尤其是安全服务内容。

7.9.12 供应链管理

本项要求包括：

a) 应确保供应商的选择符合国家有关规定；
b) **应以书面方式约定数据交换、共享的接收方对数据的保护责任，并明确数据安全保护要求。**

7.9.13 数据源管理

应通过合法正当渠道获取各类数据。

7.10 安全运维管理

7.10.1 环境管理

GB/T 22239-2019 8.1.10.1。

7.10.2 资产管理

本项要求包括：

a) GB/T 22239-2019 8.1.10.2；
b) 应建立数据资产安全管理策略，对数据全生命周期的操作规范、保护措施、管理人员职责等进行规定，包括并不限于数据采集、传输、存储、处理、交换、销毁等过程；
c) **应制定并执行数据分类分级保护策略，针对不同类别级别的数据制定相应强度的安全保护要求；**
d) **应定期评审数据的类别和级别，如需要变更数据所属类别或级别，应依据变更审批流程执行变更；**
e) 应对数据资产和**对外数据接口**进行登记管理，建立相应资产清单。

7.10.3 介质管理

本项要求包括：

a) GB/T 22239-2019 8.1.10.3；
b) 应在中国境内对数据进行清除或销毁。

7.10.4 设备维护管理

GB/T 22239-2019 8.1.10.4。

7.10.5 漏洞和风险管理

GB/T 22239-2019 8.1.10.5。

7.10.6 网络和系统安全管理

本项要求包括：

a) GB/T 22239-2019 8.1.10.6；

b) b）应建立对外数据接口安全管理机制，所有的接口调用均应获得授权和批准。

7.10.7 恶意代码防范管理

GB/T 22239-2019 8.1.10.7。

7.10.8 配置管理

GB/T 22239-2019 8.1.10.8。

7.10.9 密码管理

GB/T 22239-2019 8.1.10.9。

7.10.10 变更管理

GB/T 22239-2019 8.1.10.10。

7.10.11 备份与恢复管理

GB/T 22239-2019 8.1.10.11。

7.10.12 安全事件处置

GB/T 22239-2019 8.1.10.12。

7.10.13 应急预案管理

GB/T 22239-2019 8.1.10.13。

7.10.14 外包运维管理

GB/T 22239-2019 8.1.10.14。

8 第四级安全要求

8.1 安全物理环境

8.1.1 物理位置选择

GB/T 22239-2019 9.1.1.1。

8.1.2 物理访问控制

GB/T 22239-2019 9.1.1.2。

8.1.3 防盗窃和防破坏

GB/T 22239-2019 9.1.1.3。

8.1.4 防雷击

GB/T 22239-2019 9.1.1.4。

8.1.5 防火

GB/T 22239-2019 9.1.1.5。

8.1.6 防水和防潮

GB/T 22239-2019 9.1.1.6。

8.1.7 防静电

GB/T 22239-2019 9.1.1.7。

8.1.8 温湿度控制

GB/T 22239-2019 9.1.1.8。

8.1.9 电力供应

GB/T 22239-2019 9.1.1.9。

8.1.10 电磁防护

GB/T 22239-2019 9.1.1.10。

8.1.11 基础设施位置

应保证承载大数据存储、处理和分析的设备机房位于中国境内。

8.2 安全通信网络

8.2.1 网络架构

本项要求包括：

a) GB/T 22239-2019 9.1.2.1；
b) 应保证大数据平台不承载高于其安全保护等级的大数据应用；
c) 应保证大数据平台的管理流量与系统业务流量分离。

8.2.2 通信传输

GB/T 22239-2019 9.1.2.2。

8.2.3 可信验证

GB/T 22239-2019 9.1.2.3。

8.3 安全区域边界

GB/T 22239-2019 9.1.3。

8.4 安全计算环境

8.4.1 身份鉴别

本项要求包括：

a) GB/T 22239-2019 9.1.4.1；
b) 大数据平台应能对不同客户的大数据应用进行身份鉴别；
c) 应对数据采集终端、数据导入服务组件、数据导出终端、数据导出服务组件的使用实施身份鉴别；
d) 应对向大数据系统提供数据的外部实体进行身份鉴别；
e) 大数据平台提供的各类外部调用接口应依据调用主体的操作权限进行相应强度的身份鉴别。

8.4.2 访问控制

本项要求包括：
a) GB/T 22239-2019 9.1.4.2；
b) 对外提供服务的大数据平台，平台或第三方只有在大数据应用授权下才可以对大数据应用的数据资源进行访问、使用和管理；
c) 大数据平台应提供数据分类分级标识功能；
d) 应在数据采集、传输、存储、处理、交换及销毁等各个环节，支持对数据进行分类分级处置，最高等级数据的相关保护措施不低于**第四级**安全要求，安全保护策略在各环节保持一致；
e) **大数据平台应具备设置数据安全标记功能，并基于安全标记进行访问控制；**
f) 大数据平台应对其提供的各类接口的调用实施访问控制，包括但不限于数据采集、处理、使用、分析、导出、共享、交换等相关操作；
g) 应最小化各类接口操作权限；
h) 应最小化数据使用、分析、导出、共享、交换的数据集；
i) 大数据平台应提供隔离不同客户应用数据资源的能力；
j) **应采用技术手段限制在终端输出重要数据。**

8.4.3 安全审计

本项要求包括：
a) GB/T 22239-2019 9.1.4.3；
b) 大数据平台应保证不同客户大数据应用的审计数据隔离存放，并提供不同客户审计数据收集汇总和集中分析的能力；
c) 大数据平台应对其提供的各类接口的调用情况进行审计；
d) 应保证大数据平台服务商对服务客户数据的操作可被服务客户审计。

8.4.4 入侵防范

本项要求包括：
a) GB/T 22239-2019 9.1.4.4；
b) 应对导入或者其他数据采集方式收集到的数据进行检测，避免出现恶意数据输入。

8.4.5 恶意代码防范

GB/T 22239-2019 9.1.4.5。

8.4.6 可信验证

GB/T 22239-2019 9.1.4.6。

8.4.7 数据完整性

本项要求包括：

a) GB/T 22239-2019 9.1.4.7；
b) 应采用技术手段对数据交换过程进行数据完整性检测；
c) 数据在存储过程中的完整性保护应满足数据源系统的安全保护要求。

8.4.8 数据保密性

本项要求包括：

a) GB/T 22239-2019 9.1.4.8；
b) 大数据平台应提供静态脱敏和去标识化的工具或服务组件技术；
c) 应依据相关安全策略和数据分类分级标识对数据进行静态脱敏和去标识化处理；
d) 数据在存储过程中的保密性保护应满足数据源系统的安全保护要求。

8.4.9 数据备份恢复

本项要求包括：

a) GB/T 22239-2019 9.1.4.9；
b) 备份数据应采取与原数据一致的安全保护措施；
c) 大数据平台应保证用户数据存在若干个可用的副本，各副本之间的内容应保持一致性；
d) 应提供对关键溯源数据的备份。

8.4.10 剩余信息保护

本项要求包括：

a) GB/T 22239-2019 9.1.4.10；
b) 数据整体迁移的过程中，应杜绝数据残留；
c) 大数据应用应基于数据分类分级保护策略，明确数据销毁要求和方式；
d) 大数据平台应能够根据大数据应用提出的数据销毁要求和方式实施数据销毁。

8.4.11 个人信息保护

本项要求包括：

a) GB/T 22239-2019 9.1.4.11；
b) 采集、处理、使用、转让、共享、披露个人信息应在个人信息处理的授权同意范围内；
c) 应采用措施防止在数据处理、使用、分析、导出、共享、交换等过程识别出个人身份信息。

8.4.12 数据溯源

本项要求包括：

a) 应跟踪和记录数据采集、处理、分析和挖掘等过程，保证溯源数据能重现相应过程；
b) 溯源数据应满足数据业务要求和合规审计要求；
c) **应采用技术手段保证溯源数据真实性和保密性。**

8.5 安全管理中心

8.5.1 系统管理

本项要求包括：

a) GB/T 22239-2019 9.1.5.1；

b) 大数据平台应为大数据应用提供管理其计算和存储资源使用状况的能力；
c) 大数据平台应对其提供的辅助工具或服务组件，实施有效管理；
d) 大数据平台应屏蔽计算、内存、存储资源故障，保障业务正常运行；
e) 大数据平台在系统维护、在线扩容等情况下，应保证大数据应用的正常业务处理能力。

8.5.2 审计管理

GB/T 22239-2019 9.1.5.2。

8.5.3 安全管理

GB/T 22239-2019 9.1.5.3。

8.5.4 集中管控

GB/T 22239-2019 9.1.5.4。

8.6 安全管理制度

GB/T 22239-2019 9.1.6。

8.7 安全管理机构

8.7.1 岗位设置

GB/T 22239-2019 9.1.7.1。

8.7.2 人员配备

GB/T 22239-2019 9.1.7.2。

8.7.3 授权和审批

本项要求包括：

a) GB/T 22239-2019 9.1.7.3；
b) 数据的采集应获得数据源管理者的授权，确保数据收集最小化原则；
c) 应建立数据集成、分析、交换、共享及公开的授权审批控制流程，依据流程实施相关控制并记录过程；
d) 应建立跨境数据的评估、审批及监管控制流程，并依据流程实施相关控制并记录过程。

8.7.4 沟通和合作

GB/T 22239-2019 9.1.7.4。

8.7.5 审核和检查

GB/T 22239-2019 9.1.7.5。

8.8 安全管理人员

GB/T 22239-2019 9.1.8。

8.9 安全建设管理

8.9.1 定级和备案

GB/T 22239-2019 9.1.9.1。

8.9.2 安全方案设计

GB/T 22239-2019 9.1.9.2。

8.9.3 产品采购和使用

GB/T 22239-2019 9.1.9.3。

8.9.4 自行软件开发

GB/T 22239-2019 9.1.9.4。

8.9.5 外包软件开发

GB/T 22239-2019 9.1.9.5。

8.9.6 工程实施

GB/T 22239-2019 9.1.9.6。

8.9.7 测试验收

GB/T 22239-2019 9.1.9.7。

8.9.8 系统交付

GB/T 22239-2019 9.1.9.8。

8.9.9 等级测评

GB/T 22239-2019 9.1.9.9。

8.9.10 服务供应商选择

GB/T 22239-2019 9.1.9.10。

8.9.11 大数据服务商选择

本项要求包括：

a) 应选择安全合规的大数据平台，其所提供的大数据平台服务应为其所承载的大数据应用提供相应等级的安全保护能力；
b) 应以书面方式约定大数据平台提供者的权限与责任、各项服务内容和具体技术指标等，尤其是安全服务内容。

8.9.12 供应链管理

本项要求包括：

a) 应确保供应商的选择符合国家有关规定；
b) 应以书面方式约定数据交换、共享的接收方对数据的保护责任，并明确数据安全保护要求。

8.9.13 数据源管理

应通过合法正当渠道获取各类数据。

8.10 安全运维管理

8.10.1 环境管理

GB/T 22239-2019 9.1.10.1。

8.10.2 资产管理

本项要求包括：

a) GB/T 22239-2019 9.1.10.2；
b) 应建立数据资产安全管理策略，对数据全生命周期的操作规范、保护措施、管理人员职责等进行规定，包括并不限于数据采集、传输、存储、处理、交换、销毁等过程；
c) 应制定并执行数据分类分级保护策略,针对不同类别级别的数据制定相应强度的安全保护要求；
d) 应定期评审数据的类别和级别，如需要变更数据所属类别或级别，应依据变更审批流程执行变更；
e) 应对数据资产和对外数据接口进行登记管理，建立相应资产清单。

8.10.3 介质管理

本项要求包括：

a) GB/T 22239-2019 9.1.10.3；
b) 应在中国境内对数据进行清除或销毁。

8.10.4 设备维护管理

GB/T 22239-2019 9.1.10.4。

8.10.5 漏洞和风险管理

GB/T 22239-2019 9.1.10.5。

8.10.6 网络和系统安全管理

本项要求包括：

a) GB/T 22239-2019 9.1.10.6；
b) 应建立对外数据接口安全管理机制，所有的接口调用均应获得授权和批准。

8.10.7 恶意代码防范管理

GB/T 22239-2019 9.1.10.7。

8.10.8 配置管理

GB/T 22239-2019 9.1.10.8。

8.10.9 密码管理

GB/T 22239-2019 9.1.10.9。

8.10.10 变更管理

GB/T 22239-2019 9.1.10.10。

8.10.11 备份与恢复管理

GB/T 22239-2019 9.1.10.11。

8.10.12 安全事件处置

GB/T 22239-2019 9.1.10.12。

8.10.13 应急预案管理

GB/T 22239-2019 9.1.10.13。

8.10.14 外包运维管理

GB/T 22239-2019 9.1.10.14。

9 第五级安全要求

略。

附 录 A
（规范性附录）
关于安全要求的选择和使用

大数据相关等级保护对象可抽象为大数据资源、大数据应用、大数据平台等三类组件，不同组件的安全关注点会有所不同。大数据资源的保护由大数据平台和大数据应用提供，下表A.1给出了大数据应用和大数据平台应实现的安全控制点及相关要求项。

表A.1 不同组件应实现的安全保护要求

分类	安全控制点	要求项	组件
安全物理环境	物理位置选择	本控制点全部要求项	大数据平台
	物理访问控制	本控制点全部要求项	大数据平台
	防盗窃和防破坏	本控制点全部要求项	大数据平台
	防雷击	本控制点全部要求项	大数据平台
	防火	本控制点全部要求项	大数据平台
	防水和防潮	本控制点全部要求项	大数据平台
	防静电	本控制点全部要求项	大数据平台
	温湿度控制	本控制点全部要求项	大数据平台
	电力供应	本控制点全部要求项	大数据平台
	电磁防护	本控制点全部要求项	大数据平台
	基础设施位置	本控制点全部要求项	大数据平台
安全通信网络	网络架构	本控制点全部要求项	大数据平台

分类	安全控制点	要求项	组件
	通信传输	本控制点全部要求项	大数据平台
	可信验证	本控制点全部要求项	大数据平台
安全区域边界	边界防护	本控制点全部要求项	大数据平台
	访问控制	本控制点全部要求项	大数据平台
	入侵防范	本控制点全部要求项	大数据平台
	可信验证	本控制点全部要求项	大数据平台
	恶意代码防范	本控制点全部要求项	大数据平台
	安全审计	本控制点全部要求项	大数据平台
安全计算环境	身份鉴别	a）GB/T 22239-2019 *.1.4.1；	大数据应用、大数据平台
		大数据平台应能对不同客户的大数据应用进行身份鉴别；	大数据平台
		应对数据采集终端、数据导入服务组件、数据导出终端、数据导出服务组件的使用实施身份鉴别；	大数据应用、大数据平台
		应对向大数据系统提供数据的外部实体进行身份鉴别；	大数据应用、大数据平台
		大数据平台提供的各类外部调用接口应依据调用主体的操作权限进行相应强度的身份鉴别。	大数据平台
	访问控制	a）GB/T 22239-2019 *.1.4.2；	大数据应用、大数据平台
		应采取技术手段对数据采集终端、数据导入服务组件、数据导出终端、数据导出服务组件进行限制。	大数据应用、大数据平台
		对外提供服务的大数据平台，平台或第三方只有在大数据应用授权下才可以对大数据应用的数据资源进行访问、使用和管理；	大数据平台
		大数据平台应提供数据分类分级标识功能；	大数据平台
		应在数据采集、传输、存储、处理、交换及销毁等各个环节，支持对数据进行分类分级处置，最高等级数据的相关保护措施不低于第*级安全要求，安全保护策略在各环节保持一致；	大数据应用、大数据平台
		大数据平台应具备设置数据安全标记功能，并基于安全标记进行访问控制；	大数据平台

分类	安全控制点	要求项	组件
		大数据平台应对其提供的各类接口的调用实施访问控制，包括但不限于数据采集、处理、使用、分析、导出、共享、交换等相关操作；	大数据平台
		应最小化各类接口操作权限；	大数据应用、大数据平台
		应最小化数据使用、分析、导出、共享、交换的数据集；	大数据应用、大数据平台
		大数据平台应提供隔离不同客户应用数据资源的能力；	大数据平台
		应采用技术手段限制在终端输出重要数据。	大数据应用、大数据平台
	安全审计	a）GB/T 22239-2019 *.1.4.3；	大数据应用、大数据平台
		大数据平台应保证不同客户大数据应用的审计数据隔离存放，并提供不同客户审计数据收集汇总和集中分析的能力。	大数据平台
		大数据平台应对其提供的各类接口的调用情况进行审计；	大数据平台
		应保证大数据平台服务商对服务客户数据的操作可被服务客户审计。	大数据平台
	入侵防范	本控制点全部要求项	大数据应用、大数据平台
	恶意代码防范	本控制点全部要求项	大数据应用、大数据平台
	可信验证	本控制点全部要求项	大数据应用、大数据平台
	数据完整性	a）GB/T 22239-2019 *.1.4.7；	大数据应用、大数据平台
		应采用技术手段对数据交换过程进行数据完整性检测；	大数据应用、大数据平台
		数据在存储过程中的完整性保护应满足数据源系统的安全保护要求。	大数据应用、大数据平台
	数据保密性	a）GB/T 22239-2019 *.1.4.8；	大数据应用、大数据平台
		大数据平台应提供静态脱敏和去标识化的工具或服务组件技术；	大数据平台
		应依据相关安全策略和数据分类分级标识对数据进行静态脱敏和去标识化处理；	大数据应用、大数据平台
		数据在存储过程中的保密性保护应满足数据源系统的安全保护要求。	大数据应用、大数据平台

分类	安全控制点	要求项	组件
	数据备份恢复	a）GB/T 22239-2019 *.1.4.9；	大数据资源、大数据应用、大数据平台
		备份数据应采取与原数据一致的安全保护措施；	大数据资源、大数据应用、大数据平台
		大数据平台应保证用户数据存在若干个可用的副本，各副本之间的内容应保持一致性；	大数据平台
		应提供对关键溯源数据的备份。	大数据平台
	剩余信息保护	a） GB/T 22239-2019 *.1.4.10；	大数据应用、大数据平台
		数据整体迁移的过程中，应杜绝数据残留；	大数据平台
		大数据应用应基于数据分类分级保护策略，明确数据销毁要求和方式；	大数据应用
		大数据平台应能够根据大数据应用提出的数据销毁要求和方式实施数据销毁。	大数据平台
	个人信息保护	本控制点全部要求项	大数据应用、大数据平台
	数据溯源	本控制点全部要求项	大数据应用、大数据平台
安全管理中心	系统管理	本控制点全部要求项	大数据平台
	审计管理	本控制点全部要求项	大数据应用、大数据平台
	安全管理	本控制点全部要求项	大数据应用、大数据平台
	集中管控	本控制点全部要求项	大数据平台
安全管理制度	安全策略	本控制点全部要求项	大数据应用、大数据平台
	管理制度	本控制点全部要求项	大数据应用、大数据平台
	制定和发布	本控制点全部要求项	大数据应用、大数据平台
	评审和修订	本控制点全部要求项	大数据应用、大数据平台
安全管理机构	岗位设置	本控制点全部要求项	大数据应用、大数据平台
	人员配备	本控制点全部要求项	大数据应用、大数据平台
	授权和审批	本控制点全部要求项	大数据应用、大数据平台
	沟通和合作	本控制点全部要求项	大数据应用、大数据平台
	审核和检查	本控制点全部要求项	大数据应用、大数据平台
安全管理人员	人员录用	本控制点全部要求项	大数据应用、大数据平台
	人员离岗	本控制点全部要求项	大数据应用、大数据平台
	安全意识教育和培训	本控制点全部要求项	大数据应用、大数据平台
	外部人员访问管理	本控制点全部要求项	大数据应用、大数据平台
安全建设管理	定级和备案	本控制点全部要求项	大数据应用、大数据平台
	安全方案设计	本控制点全部要求项	大数据应用、大数据平台

分类	安全控制点	要求项	组件
	产品采购和使用	本控制点全部要求项	大数据应用、大数据平台
	自行软件开发	本控制点全部要求项	大数据应用、大数据平台
	外包软件开发	本控制点全部要求项	大数据应用、大数据平台
	工程实施	本控制点全部要求项	大数据应用、大数据平台
	测试验收	本控制点全部要求项	大数据应用、大数据平台
	系统交付	本控制点全部要求项	大数据应用、大数据平台
	等级测评	本控制点全部要求项	大数据应用、大数据平台
	服务供应商选择	a) GB/T 22239-2019 *.1.9.10。	大数据应用、大数据平台
		应选择安全合规的大数据平台，其所提供的大数据平台服务应为其所承载的大数据应用提供相应等级的安全保护能力。	大数据应用
		应以书面方式约定大数据平台提供者的权限与责任、各项服务内容和具体技术指标等，尤其是安全服务内容；	大数据应用
		应以书面方式约定数据交换、共享的接收方对数据的保护责任，并明确数据安全保护要求。	大数据应用、大数据平台
	供应链管理	本控制点全部要求项	大数据应用、大数据平台
	数据源管理	本控制点全部要求项	大数据应用、大数据平台
安全运维管理	环境管理	本控制点全部要求项	大数据平台
	资产管理	本控制点全部要求项	大数据应用、大数据平台
	介质管理	本控制点全部要求项	大数据应用、大数据平台
	设备维护管理	本控制点全部要求项	大数据平台
	漏洞和风险管理	本控制点全部要求项	大数据应用、大数据平台
	网络与系统安全管理	本控制点全部要求项	大数据平台
	恶意代码防范管理	本控制点全部要求项	大数据应用、大数据平台
	配置管理	本控制点全部要求项	大数据应用、大数据平台
	密码管理	本控制点全部要求项	大数据应用、大数据平台
	变更管理	本控制点全部要求项	大数据应用、大数据平台
	备份与恢复管理	本控制点全部要求项	大数据应用、大数据平台
	安全事件处置	本控制点全部要求项	大数据应用、大数据平台
	应急预案管理	本控制点全部要求项	大数据应用、大数据平台
	外包运维管理	本控制点全部要求项	大数据应用、大数据平台

参 考 文 献

[1] NIST Special Publication 800-53 联邦信息系统推荐性安全控制措施

[2] NIST Special Publication 1500-4 DRAFT NIST Big Data Interoperability Framework: Volume 4, Security and Privacy

[3] ENISA Big Data Security：Good Practices and Recommendations on the Security and Resilience of Big Data Services

[4] CSA Big Data Working Group：Expanded Top Ten Big Data Security and Privacy Challenges

[5] CSA Big Data Security and Privacy Handbook: 100 Best Practices in Big Data Security and Privacy

[6] T-REC-Y.3600-201511Big data—Cloud computing based requirements and capabilities

[7] Federal Trade Commission, Data Brokers: A Call for Transparency and Accountability

[8] 大数据标准化白皮书-中电研究院

[9] 大数据安全管理自评估指南