《信息安全技术 网络安全等级保护大数据基本要求》

编制说明

一、工作简况

1、任务来源

为配合国家网络安全等级保护制度 2.0 全面推进，加强对大数据等级保护对象的安全保护指导工作，由中关村信息安全测评联盟组织发起，公安部信息安全等级保护评估中心为标准编制牵头单位，中关村信息安全测评联盟为项目归口管理单位，会同国家信息中心、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，共同编制《信息安全技术 网络安全等级保护大数据基本要求》（简称“大数据基本要求”）。

本标准基于《GB/T 22239-2019 信息安全技术 网络安全等级保护基本要求》，指导大数据等级保护对象的网络运营者如何开展相应保护的具体细化和扩展标准，对开展大数据等级保护对象的安全保护工作具有重要的指导作用。

2、编制背景

大数据蕴含着巨大价值，小则影响业务决策，大则关乎国家安全、社会稳定、公众利益，随着大数据从技术走向商业、从理论迈向实践的步伐越来越大，大数据安全成为大数据发展的一发千钧之力。习近平总书记强调，要重视数据安全，要依法加强对大数据的管理，坚持鼓励支持和规范发展并行，坚持政策引导和依法管理并举。面对数据 V 特征带来了安全影响，大数据技术迅速迭代，攻击手段日新月异，而大数据及大数据系统的安全防护能力参差不齐的安全现状，迫切需要制定完善权威的、系统的大数据安全标准规范，合理分配资源保护大数据资源、大数据平台和大数据应用，指导网络运营者开展大数据等级保护对象的安全建设、安全运维和安全管理。

本标准在《信息安全技术 网络安全等级保护基本要求》（以下简称“基本要求”）提出的通用安全基线的基础上，对大数据资源及大数据应用、大数据平台方面的安全保护要求进行细化和扩展，指导全生命周期的数据安全保护，指导分等级的非涉密大数据等级保护对象的安全建设、安全运维和测试评估，为网络安全等级保护制度在大数据领域的推广和落实奠定基础，并为信息安全监管职能部门、测评服务机构、主管部门及运营使用者对大数据的安全保护、等级测评、监督检查等提供参考依据。

3、主要工作过程

2019 年 6 月，受中关村信息安全测评联盟委托，成立网络安全等级保护大数据基本要求编制组，完成基本文档基础架构及编制成员任务分工。

2019 年 6 月—7 月，编制组根据分工进行内容编制，并形成《网络安全等级保护大数据基本要求》合稿。

2019 年 7 月，经讨论组对《网络安全等级保护大数据基本要求》合稿讨论，编制组根据讨论意见对文本进行修订、完善，形成《网络安全等级保护大数据基本要求》初稿。

2019 年 8 月上旬，《网络安全等级保护大数据基本要求》初稿向等级保护测评机构、业内专家征求意见。

2019 年 9 月下旬，编制组根据反馈的征求意见进一步完善《网络安全等级保护大数据基本要求》初稿，并进行专题研讨。

2019 年 10 月，根据研讨会意见，对文档的结构、内容进行修订、完善，形成了《信息安全技术 网络安全等级保护大数据基本要求》征求意见稿，并于 10 月中旬向标委会秘书处提交征求意见稿及编制说明。

4、标准起草单位及人员

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：

公安部信息安全等级保护评估中心负责组织《网络安全等级保护大数据基本要求》标准文本的起草，按照团体标准报批要求，分阶段完成征求意见稿、送审稿、报批稿和其他相关材料，负责收集各起草单位的指导意见，进行汇总、分析，完成全文的编写、统稿工作。

二、标准主要内容及依据

标准编制组前期深入研究大数据保护对象的特点，结合大数据现有技术的发展水平、系统形态和安全防护需求，分析不同大数据网络运营者需要对抗的安全威胁，以及应采取的安全机制或措施，明确不同安全保护等级大数据对象应实现的安全保护目标。通过吸取国际、国内最先进的信息安全技术和经验，结合编制组成员单位既有工作经验，编制组充分认识到大数据的安全保护工作包括两方面的内容，一是对数据资源实施全生命周期的安全保护，二是结合大数据技术的特点对大数据系统（大数据平台、大数据应用）实施安全保护。

标准针对数据生命周期提出相应要求，如“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、存储、处理、应用、流动、销毁等过程；”，“涉及重要数据接口、重要服务接口的调用，应实施访问控制，包括但不限于数据处理、使用、分析、导出、共享、交换等相关操作。”等，编制组认为，只有实现对数据全生命周期的安全保护才能真正达到保护数据安全的目的。

此外，编制组研究构建大数据生命周期模型，分析生命周期各环节的活动及安全目标，

细化分解各环节的威胁源、威胁对象和风险场景，研究落实每一环节数据安全保护的具体安全技术和管理措施。同时，编制组在对大数据平台、大数据应用的安全风险分析基础上，充分识别大数据平台和大数据应用应承担的数据安全保护职责以及供应链上彼此的安全关系，划分数据采集、交换、共享等数据流动环节数据安全保护职责关系，重点关注个人敏感信息、重要业务数据、跨境数据、溯源数据等重要数据的安全保护，明确采用大数据技术的大数据平台和应用的特殊安全保护需求，传承《基本要求》的标准定位和描述模型，在《基本要求》提出的安全保护基线的基础上，针对大数据安全保护对象提出细化和扩展的安全要求。

具体内容包括：

1) 第一章 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，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。

2) 第二章 规范性引用文件

本标准中引用了最新版国标，以保证本标准条款的可依性和可行性。根据工作组会议讨论决定，规范性引用文件严格按照《标准化工作导则第 1 部分：标准结构和编写》GB/T1.1-2009 要求进行逐条核对，并将本标准引用的标准全部列入。

3) 第三章 术语和定义

本章对文中会使用的术语进行了定义，对后续章节内容描述提供了术语支持。

4) 第四章 概述

本章对于标准条款的约束对象——大数据等级保护对象的构成进行了描述，并将大数据相关的所有定级对象称为“大数据”系统。

5) 第五章到第九章

本部分为标准的主体内容，根据大数据产品和技术现状，参照通用要求的级差特点和相应等级保护能力，提出提出了第一级到第五级的各级别基线要求，包括了大数据等级保护对象应实现的所有安全保护要求。

6) 附录 A 关于安全要求的选择和使用

由于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，每类组件应实现的安全保护要求也会不同，尤其是大数据定级对象可能为其中的一类或多类组件，为便于网络运营者的落地实施，给出了不同类组件应该落实的安全保护要求。

标准使用需要配合《基本要求》，大数据系统需首先满足《基本要求》提出的通用安全要求，然后满足本标准针对大数据系统提出的扩展的安全要求。

三、与相关法律法规及国家有关规定、国内相关标准的关系

1) 与《基本要求》的关系

《基本要求》中资料性附录包括“大数据应用场景说明”，从大数据系统保护的角度提出大数据安全保护要求，但是标准本身并未给出数据资源安全保护方面的指导和要求，在大数据资源安全保护方面存在短板，等级保护制度作为我国网络安全保护的基本制度要求，有责任、有义务针对大数据保护对象提出全面的大数据安全保护要求。本标准将覆盖大数据安全保护，包括大数据资源和大数据系统的安全保护，实现二者有机结合。同时，“大数据应用场景说明”仅作为资料性的参考附录，从等保工作推进而言，力度显然也有所欠缺，目前《基本要求》刚刚发布，修订工作最快也只能明年启动，对于等级保护工作的工作指导，迫切需要先推出团体标准。在团标发布后，通过测评实践，不断检验标准的有效性，成熟后进行国标修订工作。

2) 和其他国标的关系

编制组密切关注国标的工作进展，积极参与其他标准的编制工作，目前比较已发布和在研国家标准中，仅 GB/T 35274-2017《信息安全技术 大数据服务安全能力要求》与标准的使用范围有部分重合，但该标准仅针对大数据平台提供者对外提供大数据服务这一特殊场景，编制组认为目前大数据相关的生态角色较多，大数据应用场景类型多样，该标准对于全面指导大数据应用的安全保护，显然无法满足需要。

四、知识产权情况说明

本标准不涉及专利问题。

五、与现行相关法律、法规、规章及相关标准的协调性

本标准符合我国相关的现行法律、法规和规章，为《网络安全法》等落地提供指导。同时，本标准是在《基本要求》的基础上进行的细化和扩展，与国标保持一致。

六、重大分歧意见的处理经过和依据

本标准起草过程中无重大分歧意见。

七、贯彻标准的要求和措施建议

该标准作为《基本要求》大数据部分的扩展，将依托等级保护现有的体系，其宣贯、培训和应用，将与现有的等保体系保持一致，本标准成熟后，启动国标的修订工作。

八、其它应予说明的事项

无。

《信息安全技术 网络安全等级保护大数据基本要求》标准编制工作组