ISSN:2790-1688 Volume-7-(2023)

Research and Construction of Government Data Security System Based on Hierarchical Protection

Min Du[1, 2, a], Guochao Hu[2, 3, b] and Xu Zhang[2, c]

[1] School of Cyberspace Security, Beijing Institute of Technology, China

[2] The 15th Research Institute of China Electronics Technology Group Corporation, China

[3] U University of Science and Technology of China, School of Cyberspace Security, China

[a] dumin912@163.com, [b] hugc_x@126.com, [c] zhangxujason@126.com

Abstract. This article, starting from the background and requirements of government data security system construction, based on the data security protection requirements of the Hierarchical Protection 2.0 series standards (referred to as " Hierarchical Protection 2.0"), delves into the construction approach of the data security system. It elaborates on the construction plan of the government data security system and data security protection strategies, with a focus on aspects like organizational structure, classification and grading, lifecycle, and technical system. This aims to meet the confidentiality, availability, and integrity requirements of data and provide robust support for data security protection in information systems within the field of electronic government.

Keywords: government data; data security protection system; classification and grading; data lifecycle protection.

1. Introduction

In the context of digital transformation, with the continuous and deepening application of new technologies such as artificial intelligence and big data, data, as an essential production factor, has become one of the key drivers promoting the development of e-government and technological innovation [1]. With the opening and sharing of government data, a range of data security issues such as data leaks, data loss, unauthorized access, data tampering, and violations of user privacy have become increasingly prevalent in the complex network environment [2].

Since 2021, China has successively introduced a series of relevant laws and regulations, including the promulgation and implementation of the "Data Security Law of the People's Republic of China" (referred to as the "Data Security Law"), the "Personal Information Protection Law of the People's Republic of China" (referred to as the "Personal Information Protection Law"), the "Regulations on the Security Protection of Key Information Infrastructure," and the "Measures for Cybersecurity Review," raising the protection of data security to historic heights in the country. As electronic government information systems that carry the personal information of Chinese citizens and important national data have developed over the years, they have formed large and complex databases. Therefore, ensuring the confidentiality, integrity, and availability of government data while fully harnessing its value has become a topic of close attention. This article aims to investigate the construction and practice of a government data security system, meeting the requirements of implementing relevant laws and regulations, overcoming key challenges in the field of data security, identifying private data assets, conducting data security classification and grading, analyzing data security construction requirements, establishing data security protection strategies, and enhancing the technical system of government data security. This is to effectively ensure the security of government data asset management and usage.

2. The Importance of Government Data Security System Construction

Government data elements, as the core engine in the process of digital government, are crucial for national security and economic and social development. Through research and analysis, it has been found that industries such as finance, telecommunications, and power have made

forward-looking explorations in the construction of data security systems. However, the maturity of data security capabilities in the government sector is generally low, and systematic data security work has not yet been initiated. Challenges that persist include the lack of clear authority and responsibility for data security organization management, data classification and grading, data anonymization, and insufficiently standardized requirements for data security technology protection. In the face of an increasingly severe data security landscape, government agencies and departments urgently need to establish a comprehensive data security system in accordance with relevant laws and regulations. This is to ensure efficient and secure data sharing and utilization, fully unlock and harness the potential of data elements, and support the high-quality development of government services.

The opening and sharing of government data have become important measures for government agencies to adapt to the changing roles and technological innovations in the context of big data development. This allows the full realization of the value of data, but it also brings forth data security issues. Thanks to the enactment of the "Data Security Law" and the implementation of the Hierarchical Protection 2.0, the strategic framework for data security system construction has become clear. This involves taking necessary measures to ensure that data is effectively protected and used lawfully, while also having the capability to maintain a continuous state of security [3]. Generally, the establishment of a government data security system involves two main aspects. First, there are requirements for data security protection technology, which cover critical points in the entire data processing lifecycle, including data collection, transmission, storage, usage, sharing, and disposal. This is achieved through the implementation of technology measures such as identity authentication, data access control, data encryption, data transmission protection, data leakage prevention, and data auditing to ensure the security protection and management of data. The second aspect involves security requirements for the content of data itself. This considers the data assets themselves and, in conjunction with the content, policies, and attributes of the data, employs techniques and management measures such as classification, data labeling, and data anonymization to ensure the security of the data.

3. Government Data Security System Architecture

3.1 The requirements of security levels for data safety and risk analysis

Network security level protection refers to the classification of information and its carriers based on their importance for protection [4]. Hierarchical Protection 2.0 is a set of legal and regulatory requirements implemented in China for information security and management. It aims to maintain national information security and comprehensively establish a protective information system [5]. Hierarchical Protection 2.0 imposes specific constraints on data security in terms of both technical security requirements and management safety requirements. This primarily includes aspects like data confidentiality, integrity, data backup, data recovery, and personal sensitive information protection [6]. Hierarchical Protection 2.0 has different requirements for data security at levels 1 to 5, with higher levels demanding greater security measures [7]. This article takes Level 3 protection requirements as an example and explores the construction of the data security system, taking into account the characteristics of networks and data in the government sector.

Data has risen to become a new factor of production, deeply integrating with various government application systems. While data assets are unlocking their value, the scope of data security is continuously expanding across three layers: the security of the data itself, security throughout the data lifecycle activities, and security of the data-supporting infrastructure. In foreign contexts, the U.S. Department of Defense and the National Security Agency have started using "Information Assurance (IA) [8]", and security attributes have extended to include confidentiality, integrity, availability, authenticity, and non-repudiation. As the situation evolves, in the ongoing process of unlocking the sustained value of government data, data security risks still present significant challenges. The security risks of government data mainly include the following four aspects.

- Unclear data asset inventory;
- Complex information system architecture;
- Inadequate security protection technology capability;
- Insufficient data security management.

3.2 Government Data Security System

In response to the new problems and challenges posed by data security assurance, and taking into account the existing practical experience in the construction of data security systems in government departments, as well as the top-level design of the national big data strategy, the focus is on the entire chain of activities and various stakeholders involved in the data lifecycle. This includes aspects such as data classification and grading protection, innovative management mechanisms, and the enhancement of technical capabilities. The objective is to establish a secure technical capability and management system throughout the entire data element process and all stages. This article discusses the construction and practice of the government data security protection system. In line with the goals and targets of government data security protection, and considering the nature of data content itself, data assets, data security protection technologies, and data management, the article designs a data security system framework that complies with Hierarchical Protection 2.0 requirements. This framework comprises five security domains: data security organization, data security management, personnel capabilities, data lifecycle security, and general data security. In the actual process of building and operating a data security system, government departments can use the practical experience in this article and employ a continuous optimization methodology to form a closed-loop system, encompassing planning, execution, checking, and optimization.

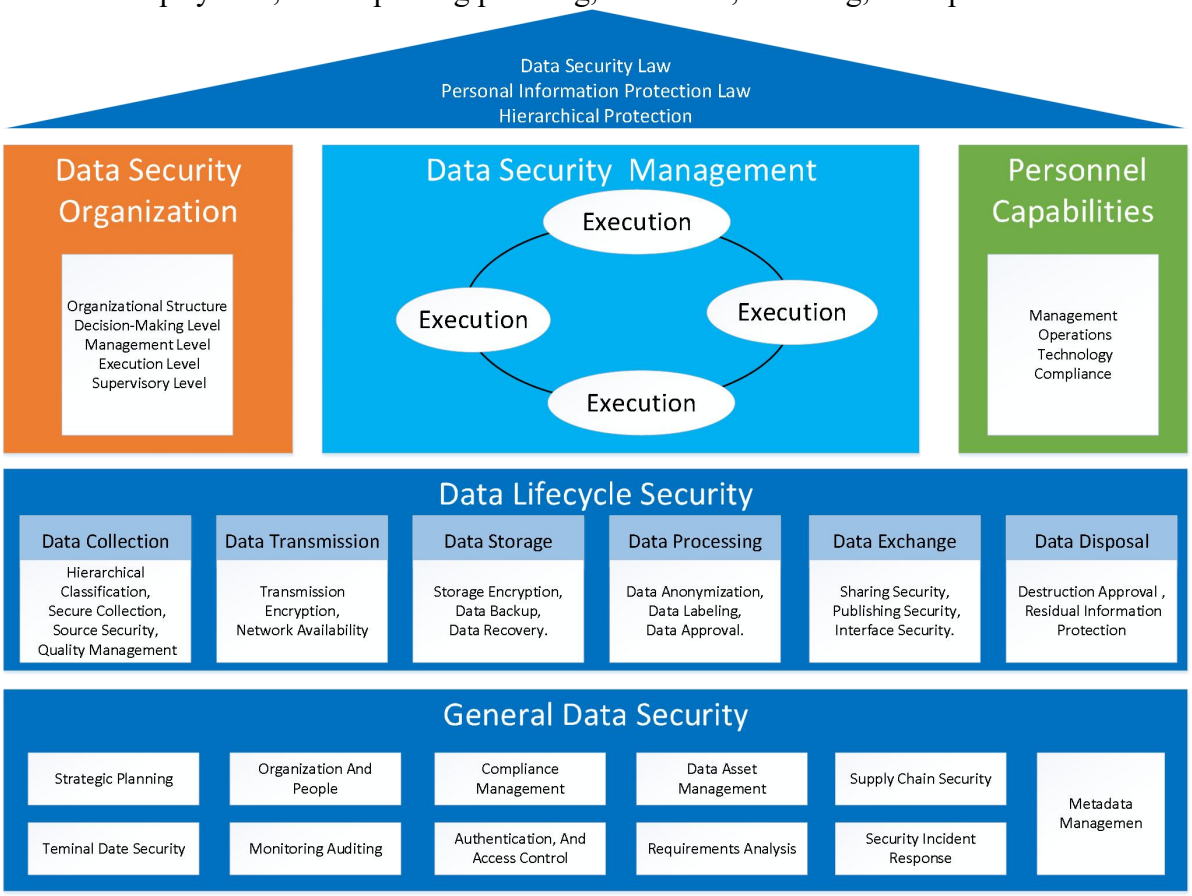

Fig. 1 Government data security system

The establishment of a data security organization should begin with constructing an organizational framework, ensuring that this framework is practical and scientifically designed to support government operations. Next, it is essential to clarify the roles and responsibilities of

decision-makers, managers, implementers, supervisors, employees, and partners. Finally, the effectiveness of communication and coordination within the data security organization in government departments should be ensured.

In terms of building the capabilities of data security personnel, it is necessary to ensure that the individuals responsible for data security possess the necessary skills to meet security objectives. This includes a solid understanding of data-related business and expertise in data security. Additionally, there should be continuous efforts to enhance the security awareness of data security personnel and to cultivate the data security capabilities of employees in key data security positions. These capabilities primarily encompass four areas: management, operations, technology, and compliance.

Data security management primarily operates through institutional processes, including data security policies and strategies, data security regulations, lines and standards, as well as data security records and logs. The institution should clearly define control measures for critical control points in the data lifecycle.

Data lifecycle security and general data security involve 30 key data security points, and specific development requirements for each key point are presented in terms of organization, personnel, institutions, and technology.

4. Government Data Security System Construction

4.1 Organization Establishment of Data Security

Government departments need to clarify the highest decision-making body for data classification and grading and appoint a top official (usually a unit leader) to oversee the construction of the data security system. It's important to identify the department responsible for the overall management of data security system construction to unify and promote the work.

Highest Decision-Making Organization: This organization provides unified guidance and coordinates the overall work of data security system construction. Responsible Management Department: This department is responsible for the overall and centralized management of data security work. It organizes the development of unified data security regulations, strategies, and implementation details, conducts research on data security protection techniques, regularly assesses and inspects data security work, evaluates the performance of internal data security responsibilities, collaborates with higher-level departments on data security work, and organizes data security education and training. A designated individual should be responsible for managing data security work. Implementing Departments: Each business department serves as the implementing department for data security. They are responsible for carrying out the construction of their department's data security system, creating data asset lists and classification grading, and implementing data security controls.

4.2 Construction of Data Security Technology System

4.2.1 Construction of a Content-Based Data Security System

(1) Data classification

The classification of government data assets generally includes two dimensions: production systems and database systems. This article, drawing from practical experience in effective information resource planning and modeling, combines production systems and database systems to construct a government data resource repository. This repository includes basic databases and integrated databases (statistical analysis databases) and forms a unified data resource catalog, enabling global indexing and cataloged management of data. Basic data is characterized by basic common resources and shared exchange data. Integrated data (statistical analysis databases) consists of various government business analysis themes, indicators, and models resulting from data analysis

and computation. The combination of basic data and integrated data forms a government data classification catalog.

(2) Data grading

The classification of government data is based on the principles established in standards and guidelines such as the "Information Security Technology - Network Data Classification and Grading Requirements" (draft for public comments, September 2022), TC260-PG-20212A, and others. It involves an assessment and grading of the impact on personal rights, organizational interests, public interests, and national security considering unauthorized use, leakage, illegal provision, and other factors. Data classification primarily focuses on data security protection and is based on two key elements: the importance of data and the impact on the objects and the severity of harm following a security incident. Based on the basic framework for data classification, data is generally divided into four levels. When performing data classification, it is important to consider the entities affected by the impact of compromised security attributes (confidentiality, integrity, availability).

Table 1. Data grading(the four levels as an example)

Data grading	Heading	Identifi -cation	Harm and Impact Severity
Level 1	Core	DL3	Causing a severe impact on the entire society, multiple industries, and multiple organizations. Causing extremely severe disruption to the normal operation of a single organization. Inflicting serious harm to personal and property safety, as well as personal reputation.
Level 2	Important	DL2	Causing a moderate level of impact on the entire society, multiple industries, and multiple organizations. Causing severe disruption to the normal operation of a single organization. Inflicting a moderate level of harm to personal reputation.
Level 3	General	DL1	Low sensitivity, causing slight impact on the entire society, multiple industries, and multiple organizations. Causing a moderate or slight disruption to the normal operation of a single organization. Inflicting minor harm to an individual's legal rights and interests.
Level 4	Public	DL0	No impact on social order, public interests, industry development, or information subjects.

4.2.2 Construction of Data Security Technology System Based on Hierarchical Protection 2.0

Data security throughout the entire data lifecycle is at the core of data classification and control. Various data security requirements span all aspects of data management. Based on the Data Security Capability Maturity Model (DSMM), the data lifecycle is divided into six stages: collection, transmission, storage, processing, exchange, and disposal. While ensuring secure data storage, government departments have strengthened data security through technical reviews, detection, monitoring, auditing, and emergency response, enhancing technical protection throughout the entire data lifecycle. Different data levels require different security protection strategies.

(1) The data collection phase. Before initiating data collection, thorough data resource planning and requirements research are required to clarify the scope of data collection.

(2) The data transmission phase. During the data transmission stage, it is essential to implement encryption for important data content and measures for data integrity and validity checks.

(3) The data usage phase. Secure management strategies should be developed based on different government data usage scenarios, such as access, statistical analysis, visualization, etc.

(4) The data sharing phase. Establish a data sharing system that complies with the requirements of Hierarchical Protection 2.0 to ensure data classification, protection, and traceability during data sharing.

(5) The data disposal phase. Establish a data disposal mechanism that defines data disposal scenarios, methods, and approval processes, among other aspects.

4.3 Establishment of management systems and personnel training for capability building

According to national laws and regulations, security standards, and industry best practices, and in conjunction with business and data resource situations, organize each implementing department to refine data security management systems, processes, and strategies, specifying data security protection principles, methods, processes, and data security control measures requirements.

Data security personnel capabilities mainly encompass several dimensions, including data security management capabilities, data security operational capabilities, data security technical capabilities, and data security compliance capabilities.

5. Summary

In the practical process of data security system construction, in conjunction with Hierarchical Protection 2.0, significant progress has been made at the level of government data security system construction through multiple stages of development and improvement, including business analysis, requirements analysis, technical implementation, process monitoring, and closed-loop enhancement. By adopting a combination of management and technology, this experience offers valuable insights for the industry, promoting the implementation of an adaptive data security system. This, in turn, helps realize the true value of government data and facilitates the development of digital governance.

References

[1] The Central Committee of the Communist Party of China and the State Council. Opinions on Building a More Perfected System for Market-Oriented Allocation of Factors [EB/OL].(2020-04-09)[2022-08-28].http://www.gov.cn/zhengce/2020-04/09/content_5500 622. htm.

[2] Sun Xuan, Wang Huanxiao. Construction of Government Big Data Security Protection Capabilities: A Discussion from the Technical and Management Perspectives. Computer Science, 2022, 49(04): 67-73.

[3] Li Haolin. Government Data Security Protection Solutions in the Era of Big Data. China New Communication. 2023,25(10):119-121. DOI:10.3969/j.issn.1673-4866.2023.10.042.

[4] Yu, Ruli, Ma, Xianping, Yang, Ya. Improving Information System Management through Information Security Level Protection. Information and Computers, 2019(7), 196-197.

[5] Chen, Tianwen, Gao, Hongzhen. Requirements and Specific Measures for Cybersecurity Level Protection in Public Libraries. Journal of Henan Library Science, 2021, 41(5), 9-11.

[6] Ma, Li, Zhu, Guobang, Lu, Lei. Interpretation of the Standard "Basic Requirements for Cybersecurity Level Protection" (GB/T 22239-2019). Information and Network Security, 2019(2), 77-84.

[7] Shi, Yong. Exploration of Data Security Audit Methods and Content. China Internal Audit, 2021(2), 40-42.

[8] Information Assurance Technical Framework (IATF) by the U.S. National Security Agency and the NIST 800 series standards developed by the U.S. National Institute of Standards and Technology.