ICS 35.040
CCS L80

NATIONAL STANDARD OF THE PEOPLE'S REPUBLIC OF CHINA

GB/Z 30286-2013

Information security technology - Guide for the production of information system protect profile and information system security target

信息安全技术 信息系统保护轮廓和信息系统安全目标产生指南

Issued on: December 31, 2013 **Implemented on: December 31, 2013**

Issued by: State Administration for Market Regulation;
Standardization Administration of China

Table of Contents

Foreword III
Introduction IV
1 Scope 1
2 Normative references 1
3 Terms and definitions 1
4 Overview of the ISPP and the ISST 1
4.1 Purpose of the ISPP and the ISST 1
4.2 Content of the ISPP and the ISST 1
4.3 Target readers of the ISPP and the ISST 4
5 Process of producing the ISPP and the ISST 4
6 Descriptive part of the ISPP and the ISST 5
6.1 Overview 5
6.2 Identification of the ISPP and the ISST 5
6.3 Overview of the ISPP and the ISST 5
6.4 ISPP application notes 6
7 Description of the information system 6
7.1 Overview 6
7.2 Description of the mission of the information system 6
7.3 Outline description of the information system 6
7.4 Detailed description of the information system 6
8 Security assurance requirements 7
8.1 Overview 7
8.2 Identifying and stating the assumptions 7
8.3 Identifying and stating the threats 8
8.4 Identifying and determining the organizational security policy 11
8.5 Making clear the definition of the security assurance requirements 12
9 Security assurance objectives 12
9.1 Overview 12
9.2 List of threats, assumptions and organizational security policy 13
9.3 Assurance objectives of the information system environment 13
9.4 Security assurance objectives of the information system 13
10 Security assurance requirements 13

10.1 Overview 13
10.2 Security technical assurance requirements 15
10.3 Security management assurance requirements 19
10.4 Security engineering assurance requirements in the ISPP or the ISST 20
11 Outline specification of the information system 22
11.1 Overview 22
11.2 Overview of the outline specification of the information system 22
11.3 Selection of the security assurance measures 23
12 ISPP statement 24
12.1 Overview 24
12.2 ISPP reference 24
12.3 ISPP tailoring 24
12.4 ISPP additions 24
13 Conformance statement 25
13.1 Overview 25
13.2 Conformance statement of the security assurance objectives 25
13.3 Conformance statement of the security assurance requirements 27
Annex A (informative) Selection of STRs from GB/T 20274.2-2008 29
Annex B (informative) Selection of SMRs from GB/T 20274.3-2008 33
Annex C (informative) Selection of SERs from GB/T 20274.4-2008 36
Bibliography 37

Foreword

This instructional document has been drafted in accordance with the rules given in GB/T 1.1-2009. Please note that some of this document may be patentable. The issuing agencies of this document do not bear the responsibility of identifying these patents. This Guidance Document is proposed and managed by the National Technical Committee for Information Security Standardization (SAC/TC260). The main drafting of the technical guidance of this document. China Information Security Assessment Center, China Information Security Assessment Center Huazhong Assessment Center, North China Institute of Computing Technology. The main drafters of this technical paper are Jiang Changqing, Zhang Li, Yao Yi, Tong Xin, Peng Yong, Luli, Hu Weihua, Fu Min and Zhou Jin.

This guidance document is a complete set of GB/T 20274 "Information Security Technology Information System Security Assessment Framework" series of standards Guidance document for Information System Protection Profile (ISPP) and Information Systems

Security Objective (InformationSystemSecurityTarget, ISST) to provide guidance. Users of this guidance document should be familiar with GB/T 20274 series of standards. Information Security Technology Information system protection profile and information system security objectives Create a guide

1 Scope

GB/Z 30286-2013 is the Chinese national standard on information security technology - guide for the production of information system protect profile and information system security target, in the field of information technology. The /Z suffix marks it as a guiding technical document: it does not prescribe requirements that can be certified against, but sets out the technique, the method or the state of the art that the standards bodies recommend following. It was issued on 31 December 2013 by the State Administration for Market Regulation; Standardization Administration of China. As a guiding technical document it carries no separate date of entry into force: it applies from publication. Classification: ICS 35.040, CCS L80. This page is published from the official record of the standard held by the Chinese standards administration: the identification, the dates, the classification and the issuing body are taken from there. The clause text, the tables and the numeric limits are in the document itself, which is delivered complete in English translation.

This guidance document gives the process of preparing an Information Systems Protection Profile (ISPP) and Information Systems Security Objective (ISST) Write ISPP and ISST to provide guidance. This guideline is applicable to assessors applying the GB/T 20274 series of standards for information system security assurance assessment Certified evaluators who act as authenticators, system developers and so on.

2 Normative references

The following documents for the application of this document is essential. For dated references, only the dated version applies to this article Pieces. For undated references, the latest edition (including all amendments) applies to this document.

GB/T 20274.1-2006 Information Security Technology Information System Security Assessment Framework Part 1. Introduction and general model

GB/T 20274.2-2008 Information Security Technology Information System Security Assessment Framework Part 2. Technical Support

GB/T 20274.3-2008 Information Security Technology Information System Security Assessment Framework Part 3. Management assurance

GB/T 20274.4-2008 Information Security Technology Information System Security Assessment Framework Part 4. Engineering Assurance Information security technology Information security risk assessment code

3 Terms and definitions

GB/T 20274.1-2006, GB/T 20274.2-2008, GB/T 20274.3-2008, GB/T 20274.4-2008 defined Terms and definitions apply to this document.

4 ISPP and ISST overview

4.1 ISPP and ISST purposes The main purpose of GB/T 20274 series of standards is to express the requirements of security assurance of information system. There are many different kinds of information systems Each information system operates in a specific real-world environment, subject to constraints from the internal and external environment of the organization. So for different Information systems usually have different security requirements. GB/T 20274.1-2006 in ISPP and ISST to express a certain type of information systems and a specific information system security Barrier requirements. The owners of information systems use ISPP to describe the standardization, structuring and standardization of the security of a certain type of information system begging. Information system developers based on ISPP for the preparation of a specific information system corresponding ISST, describes the security of its specific user system Support requirements and fulfillment of ISPPs.

4.2 ISPP and ISST content Figure A.1 of GB/T 20274.1-2006 describes the content items required in ISPP. Table 1 is the recommended ISPP sample