

ICS 35.240  
CCS A 90

**GA**

**INDUSTRY STANDARD OF THE  
PEOPLE'S REPUBLIC OF CHINA**

**GA/T 1144-2014**

---

**Information security technology. Security technical  
requirements for unauthorized external connection monitoring  
products**

信息安全技术 非授权外联监测产品安全技术要求  
**(English Translation)**

**Issued on: January 1, 1970**

**Implemented on: January 1, 1970**

---

**Issued by: Ministry of Public Security**

## Table of Contents

|                                                       |
|-------------------------------------------------------|
| Preface                                               |
| Introduction                                          |
| 1 Scope                                               |
| 2 Normative reference document                        |
| 3 Terms and definitions                               |
| 4 Unauthorized Outside Monitoring Product Description |
| 5 Security environment                                |
| 5.1 Hypothesis                                        |
| 5.2 Threats                                           |
| 5.3 Organizational Security Strategy                  |
| 6 Safe purpose                                        |
| 6.1 Product safety objectives                         |
| 6.2 Environmental safety objectives                   |
| 7 Safety function requirements                        |
| 7.1 Controlled host management                        |
| 7.2 Unauthorized outreach monitoring                  |
| 7.3 Response processing                               |
| 7.4 Component Security                                |
| 7.5 Safety Management                                 |
| 7.6 Audit function                                    |
| 8 Security requirements                               |
| 8.1 Configuration Management                          |
| 8.2 Delivery and Operation                            |
| 8.3 Development                                       |
| 8.4 Guidance Document                                 |
| 8.5 Life cycle support                                |
| 8.6 Test                                              |
| 8.7 Assessment of vulnerability                       |

## Foreword

This standard is drafted in accordance with the rules given in GB/T 1.1-2009.

This standard is proposed by the Ministry of Public Security Network Security Bureau.

This standard by the Ministry of Public Security Information System Security Standardization Technical Committee.

The drafting of this standard. the Ministry of Public Security Computer Information System Security Product Quality Supervision and Inspection Center, the Ministry of Public Security Network Security Bureau, Xiamen City, the United States and Asia Park Branch Information Co., Ltd., the Ministry of Public Security Third Institute.

## Introduction

This standard describes in detail the assumptions, threats, and organizational security policies associated with non-authorized outreach monitoring of the product's security environment, the purpose of the outreach monitoring product and its supporting environment is to demonstrate that the safety function requirements can be traced back and covered with product safety objectives, safety objectives the ability to trace and cover security-related assumptions, threats, and organizational security policies.

The basic level of this standard refers to the GB/T 18336.3-2008 in the provisions of the EAL2 level security requirements, enhanced level in the EAL4 level Security assurance requirements, based on the vulnerability analysis requirements can be raised to attack the potential of attack.

This standard only gives the technical requirements for non-authorized outreach monitoring products to be met, but the specific technical aspects of non-authorized outreach monitoring products Technology to achieve the way, methods do not do the request.

Information Security Technology Technical requirements for non - authorized outreach monitoring product safety

## 1 Scope

This standard specifies the safety functional requirements, safety assurance requirements, and grading requirements for non-authorized outreach products.

This standard applies to the design, development and testing of unauthorized outreach monitoring products.

## 2 Normative reference documents

The following documents are indispensable for the application of this document. For dated references, only the dated edition applies to this article. For undated references, the latest edition (including all modifications) applies to this document.

Classification rules for the classification of security levels for computer information systems  
GB 17859-1999 GB/T 18336-2008 (all parts) Information technology Security technology  
Information technology security assessment criteria Information security technical  
terminology GB/T 25069-2010

## 3 Terms and definitions

GB 17859-1999, GB/T 18336-2008 (all parts) and GB/T 25069-2010 and the following terms and definitions Apply to this document.

Unauthorized outexientconnection the interconnection behavior of the protected network internal hosts in connection with unauthorized networks outside the security policy, including but not limited to dual Network card, modem, ADSL, wireless card and so on.

Proxy agent

Software program, can accept the server control, to achieve the host of non-authorized outreach behavior monitoring.

Controlled host controledhost Installed the agent, able to accept the server control of the host.

## 4 Unauthorized Outside Monitoring Product Description

Unlicensed outbound monitoring products are usually deployed in C/S mode, including servers and agents. Can be controlled by the server on the host. Issued a policy to monitor or block the host host in the security policy to allow the connection outside the non-authorized network behavior, and its timely positioning, the agent can send the monitoring results and alarm information to the server.

There are two main types of network environments for non-authorized outreach monitoring products. one is an isolated network, which is physically isolated from other networks, Usually that the network within the network through a certain way to connect to other networks that is non-authorized outreach; the second category for the controlled network, the network and other networks are logically accessible, but access to other networks is controlled and/or auditable if the hosts within the network pass