

Graded Protection of Information Security & Other Standards

Lecture 2

HCIA-Security

Prepared by
Dr. Abdelrhman Ahmed

Chapter
02

Definition

Graded protection of information and information carriers based on their importance levels

National Regulations and Requirements

No. 27 [2003] of the General Office of the CPC Central Committee Opinions for Strengthening Information Security Assurance Work

Key contents:

- Implementing the policy on graded protection of information security
- Attaching importance to information security risk assessment
- Building and improving the information security monitoring system
- Ensuring information security funds
- Improving the accountability system for information security management

Supervision by Public Security Dept



No. 66 [2004] of the Ministry of Public Security: Notice on Issuing the Implementation Opinions on the Graded Protection of Information Security

- Public security sector: supervision, inspection, and guidance of graded protection
- State secrecy departments: supervision, inspection, and guidance of classified work for graded protection
- State cryptography administration departments: supervision, inspection, and guidance of cryptography work for graded protection

Implemented by HQs and Industries



1. Public communication networks of telecom and broadcast/film/TV industries. Basic information networks such as broadcast/TV transmission networks. Important information systems of units such as Internet information service units, Internet access service units, and data centers
2. Important information systems for the production, scheduling, management, and office of railway, bank, custom, taxation, electricity, securities, insurance, diplomacy, science and technology, development reform, defense science and technology, public security, personnel/labor and social security, finance, auditing, commerce, water conservancy, land and energy resources, transportation, culture, education, statistics, industry and commerce administration, and postal sectors

Chapter
02

Significance

1. Improve protection and resource allocation

■Improving overall protection

Effectively improving overall information security assurance and resolving threats and major issues faced by information systems

■Optimizing resource allocation

Investing limited financial, material, and human resources in key areas to maximize economic benefits of security

2. Law and regulation compliance

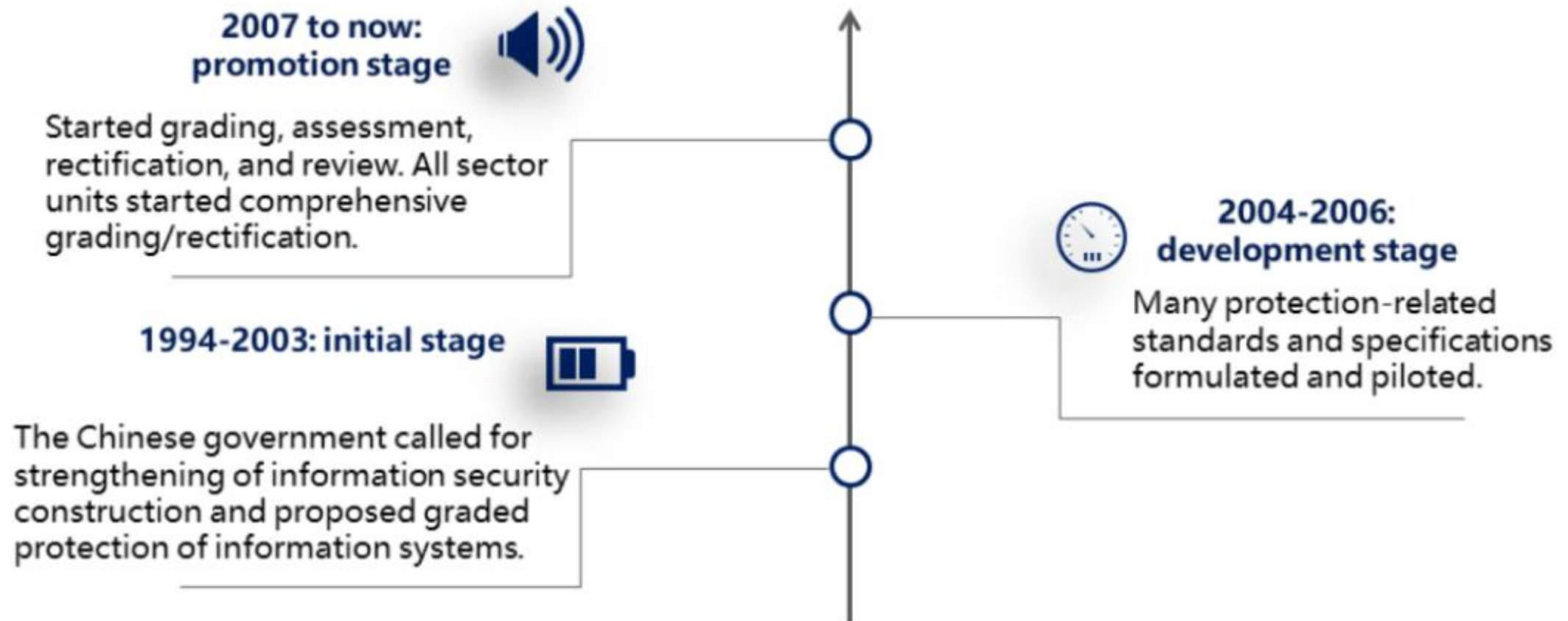
Chapter III: Network Operations Security Section 1: General Provisions

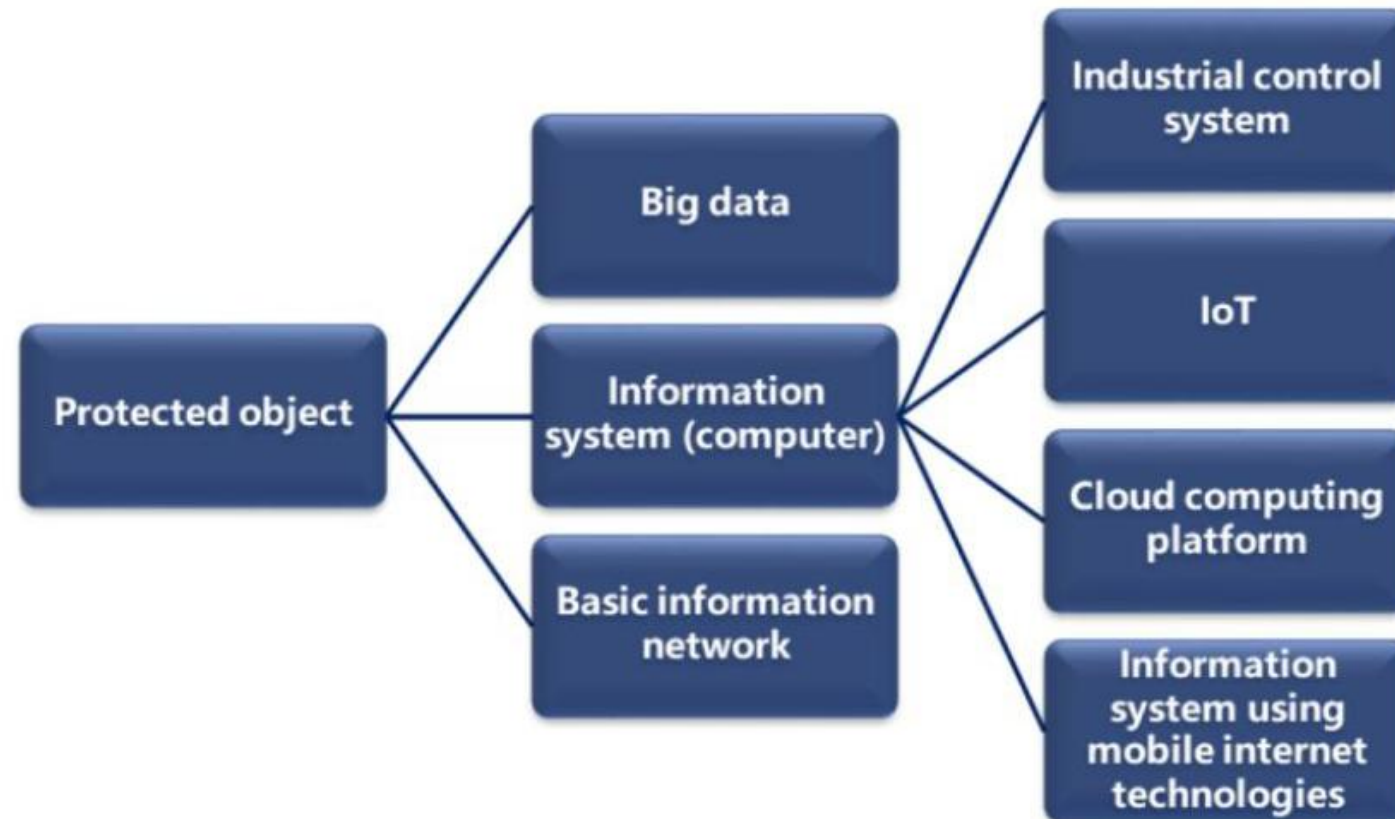
Article 21: The State implements a tiered cybersecurity protection system.

Network operators shall fulfill the following security protection duties according to the requirements of the tiered cybersecurity protection system, to ensure that networks avoid interference, damage, or unauthorized access, and to guard against network data leaks, theft, or tampering:

- Formulate internal security management systems and operating rules, determine persons responsible for cybersecurity, and implement cybersecurity protection responsibility;
- Adopt technological measures to prevent computer viruses, network attacks, network intrusions and other actions endangering cybersecurity;
- Take technological measures for monitoring and recording network operating status and cybersecurity incidents, and follow regulations to store network logs for no less than six months;
- Adopt measures such as data classification, backup of important data, and encryption;
- Fulfill other obligations as provided by law or administrative regulations.

Background & Development





Grades

- The grades are defined based on the extent of information system damage to citizens, society, and state.

Grade	Legitimate Rights and Interests of Citizens and Legal Persons	Social Order and Public Interests	National Security
I	Damage	N/A	N/A
II	Severe damage	Damage	N/A
III	/	Severe damage	Damage
IV	/	Severe damage	Severe damage
V	/	/	Severe damage

Basic Technical Requirements

- Each grade of protection has corresponding technical requirements. For example, the technical requirements for Grade III cover 5 aspects:

Physical security

App security

Data security

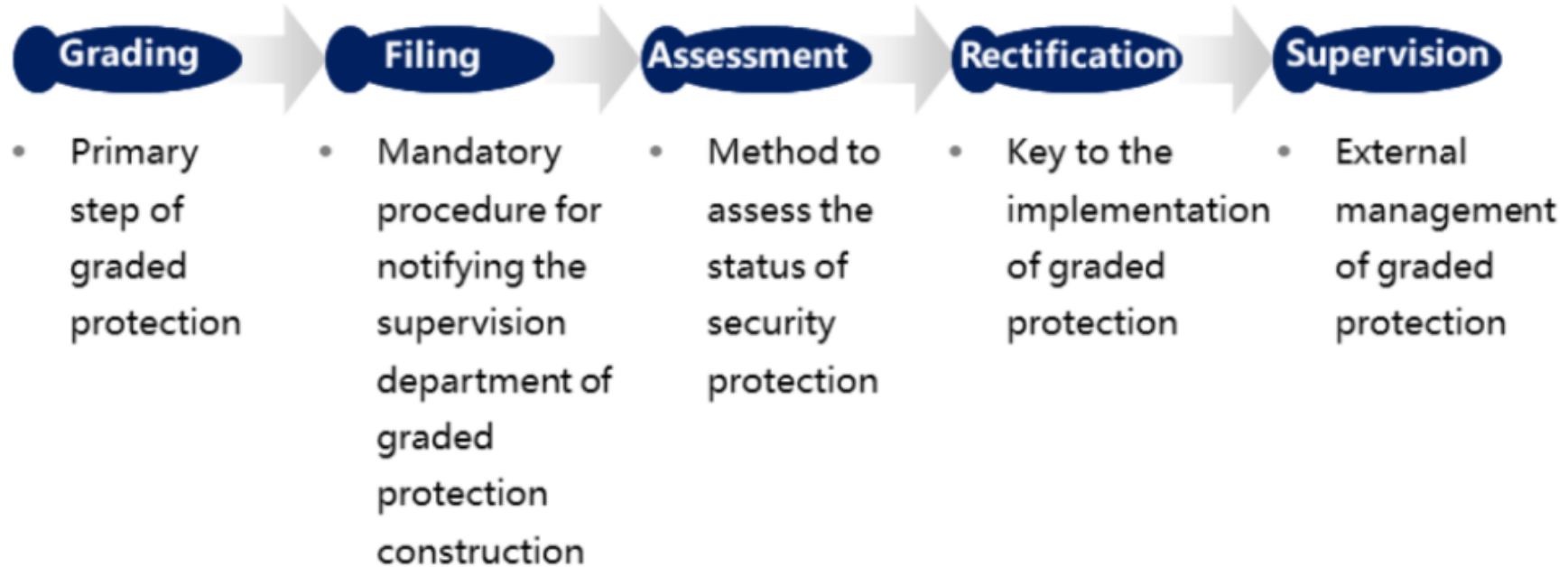
Network security

Host security

- 7 control points and 33 items:

1. Structure security (7 items)
2. Access control (8 items)
3. Security audit (4 items)
4. Boundary integrity check (2 items)
5. Intrusion prevention (2 items)
6. Malicious code program (2 items)
7. Network device protection (8 items)

Graded Protection Process



Other Standards – US - TCSEC

- Trusted Computer System Evaluation Criteria (TCSEC)
- First formal standard for computer system security evaluation
- Proposed by the Defense Science Board in 1970 and released by the United States Department of Defense in December 1985

A: Verified protection	A1	The system administrator must receive a formal security policy model from the developer. All installation operations must be performed by the system administrator. Formal documents must be available for all of these operations.
B: Mandatory protection	B1	Class-B systems are protected against access from users without security levels.
	B2	
	B3	
C: Discretionary protection	C1	Audit protection is available, and users' actions and responsibilities can be audited.
	C2	
D: Minimal protection	D1	Security protection is provided only for files and users. The most common D1 system is a local operating system or a completely unprotected network.

Chapter
02

Other Standards – Europe - ITSEC

- Information Technology Security Evaluation Criteria (ITSEC)
- Formulated by the UK, France, Germany, and the Netherlands, the ITSEC makes better progress in function flexibility and related evaluation technologies than TCSEC; applied in the military, government, and business sectors

Function		Evaluation	
Level	Description	Level	Description
		E0	Inadequate assurance
F1-F5	TCSEC D-A	E1	At this level there shall be a security target and an informal description of the architectural design of the Target of Evaluation (TOE). Functional testing shall indicate that the TOE satisfies its security target.
F6	Data and program integrity	E2	In addition to the requirements for level E1, there shall be an informal description of the detailed design. Evidence of functional testing shall be evaluated. There shall be a configuration control system and an approved distribution procedure.
F7	System availability	E3	In addition to the requirements for level E2, the source code and/or hardware drawings corresponding to the security mechanisms shall be evaluated. Evidence of testing of those mechanisms shall be evaluated.
F8	Data communication integrity	E4	In addition to the requirements for level E3, there shall be an underlying formal model of security policy supporting the security target. The security enforcing functions, the architectural design and the detailed design shall be specified in a semi-formal style.
F9	Data communication confidentiality	E5	In addition to the requirements for level E4, there shall be a close correspondence between the detailed design and the source code and/or hardware drawings.
F10	Network security including confidentiality and integrity	E6	In addition to the requirements for level E5, the security enforcing functions and the architectural design shall be specified in a formal style, consistent with the specified underlying formal model of security policy.

Other Standards – Sarbanes – Oxley Act

- Public Company Accounting Reform and Investor Protection Act of 2002, commonly called SOX.

AN ACT To protect investors by improving the accuracy and reliability of corporate disclosures made pursuant to the securities laws, and for other purposes.

--- Sarbanes-Oxley Act

What is the relationship between SOX and information security?



- Clauses in the SOX Act regarding the monitoring of contract management and enterprise operation processes can also apply to information system inspections.

Scope

- The legislation in the Sarbanes-Oxley Act (SOX) stems from a December 2001 securities scandal involving Enron, then one of the largest energy companies in the United States. The company hid massive debts that, when revealed, sent stock prices tumbling. With investor confidence "thoroughly destroyed", the United States Congress and government rapidly introduced the SOX Act. The act promised "to protect investors by improving the accuracy and reliability of corporate disclosures made pursuant to the securities laws, and for other purposes."
- The act contains the following:
 - Setting up the Public Company Accounting Oversight Board (PCAOB) to supervise registered public accounting firms
 - Strengthening auditor independence
 - Increasing the corporate responsibility for financial reports
 - Enhancing financial disclosures
 - Increasing criminal penalties



Thank You