SmartSuite

Framework / Cybersecurity / Other

China MLPS v2.0 – Levels 1–5

China's MLPS grades systems on five levels, requires filing with public security, matching safeguards and regular evaluation, with GB/T 22239-2019 as the baseline.



What it is

China's Multi-Level Protection Scheme (MLPS, also called classified protection of cybersecurity) requires network operators to grade each information system on one of five levels by the harm its destruction would cause, file the system with public security authorities, build safeguards that match its level and have the safeguards evaluated by a qualified body. "MLPS 2.0" is the 2019 generation of national standards for the scheme, led by GB/T 22239-2019, which took effect on December 1, 2019 and replaced the 2008 version.

The legal duty comes from Article 21 of the Cybersecurity Law. The Ministry of Public Security and its local public security organs administer the scheme, and the State Administration for Market Regulation and the Standardization Administration issue the GB/T standards. The 2007 Management Rules, issued by four state bodies on June 22, 2007, define the levels, filing and evaluation steps.

At a glance

PUBLISHER Ministry of Public Security (MPS); GB/T 22239-2019 issued by SAMR/SAC	TYPE Framework	VERSION MLPS 2.0 (GB/T 22239-2019 baseline; 2007 Management Rules)
EFFECTIVE December 1, 2019 (GB/T 22239-2019); 2007 Management Rules effective June 22, 2007	DOMAIN Cybersecurity	FAMILY Other
REGION China	ADOPTION MODEL Regulatory Compliance	IMPLEMENTATION COMPLEXITY High

Source: openstd.samr.gov.cn/bzgk/gb/std_list?p.p1=0&p.p90=circulation_date&p.p91=desc&p.p2=GB/T%2022239-2019

Why it matters

- **Grades follow harm, not technology** The five levels depend on the harm destruction of the system would cause to citizens' or organizations' rights, social order, the public interest or national security (Article 7 of the 2007 Rules).
- **Self-grading with review** Operators grade their own systems, a competent department verifies the grade, and systems planned for level 4 or above go to a national expert committee (Articles 6 and 10).
- **Filing with public security** Systems at level 2 and above are filed with the city-level or higher public security body within 30 days of grading or of entering operation (Article 15).
- **A fixed evaluation rhythm** Level 3 systems are evaluated and self-inspected at least yearly and level 4 at least every half year, by a qualified evaluation body (Article 14).

 © 2026 SmartSuite Inc. All rights reserved.

How SmartSuite supports MLPS 2.0

System Inventory and Grade Register

Record each system with its MLPS grade, the grading basis, the competent department's verification and the responsible person (Articles 6 and 10).

Filing Certificates and Materials

Keep the filing date, public security office, certificate and supporting materials such as the topology and product list (Articles 15 to 17).

Baseline Control Library by Level

Load the GB/T 22239-2019 technical and management requirements for each grade as controls with owners and evidence.

Evaluation Calendar and Reports

Schedule the annual level 3 or half-yearly level 4 evaluations, attach each report and track the evaluating body (Article 14).

Rectification Plans and Correction Reports

Turn evaluation and inspection findings into rectification tasks with owners and due dates, and store correction reports (Articles 14 and 20).

Inspection Readiness Reporting

Show grade, filing, evaluation and open-finding status across systems on a dashboard ahead of public security inspections.

Common framework mappings

CIS Controls v8.1 | ISO 27001:2022 | ISO 27002:2022 | ISO 27701 | MITRE ATT&CK | NIST CSF 2.0 | NIST 800-53 Rev.5

Official resources

MLPS 2.0 Classification Guide (GB/T 22240-2020)

How to grade a system into one of the five MLPS protection levels (Chinese text).

openstd.samr.gov.cn/bzgk/std/newGbInfo?hcno=63B89FFF7CC97EBBBED8A403396F0F00

MLPS 2.0 Security Design Requirements (GB/T 25070-2019)

Technical requirements for designing systems that meet the MLPS 2.0 protection levels (Chinese text).

openstd.samr.gov.cn/bzgk/std/newGbInfo?hcno=9FB6EE8597B21436D0E99BF44FD42C4D

MLPS 2.0 Implementation Guide (GB/T 25058-2019)

Guidance for organizations on implementing classified protection, from grading through evaluation (Chinese text).

openstd.samr.gov.cn/bzgk/std/newGbInfo?hcno=1E5827B2858401572CFF3A6FA711ACC9

MLPS 2.0 Baseline (GB/T 22239-2019)

The core MLPS 2.0 control baseline for each protection level, as published on the national standards platform (Chinese text).

openstd.samr.gov.cn/bzgk/std/newGbInfo?hcno=BAFB47E8874764186BDB7865E8344DAF

Frequently asked questions

What is China's Multi-Level Protection Scheme (MLPS)?

It is the scheme under which network operators in China grade each information system on five levels by the harm its destruction would cause, file it with public security, apply the matching safeguards and have them evaluated. It rests on Article 21 of the Cybersecurity Law and the GB/T national standards, led by GB/T 22239-2019.

What does MLPS 2.0 mean?

It refers to the 2019 generation of national standards for classified protection of cybersecurity. GB/T 22239-2019 took effect on December 1, 2019 and replaced the 2008 baseline, and it is supported by GB/T 28448-2019 on evaluation and GB/T 25070-2019 on security design.

Updated Oct 15, 2026 · © 2026 SmartSuite Inc. All rights reserved.

What are the five MLPS levels?

They run from level 1 to level 5 according to the harm that destruction of the system would cause: to citizens' or organizations' rights (level 1), to social order or the public interest (levels 2 to 4, in increasing gravity) and to national security (levels 3 to 5). Level 5 is the most severe (Article 7 of the 2007 Rules).

Which systems must be filed and evaluated?

Systems at level 2 and above must be filed with the city-level or higher public security body within 30 days. Level 3 systems must be evaluated at least once a year and level 4 systems at least every half year by a qualified evaluation body (Articles 14 and 15).

Who runs the MLPS?

Public security organs administer it, and they inspect level 3 systems at least yearly and level 4 systems at least every half year. The 2007 Rules were issued jointly by the Ministry of Public Security, the State Secrecy Protection Bureau, the State Encryption Management Bureau and the State Council Informatization Work Office (Article 18).

License included / downloadable: No The GB/T standards are published by China's Standardization Administration, and the full text is read through the national standards platform. The text is not included with the platform.

Full framework page and mappings: smartsuite.com/frameworks/china-mlps-2-0-multi-level-protection-scheme