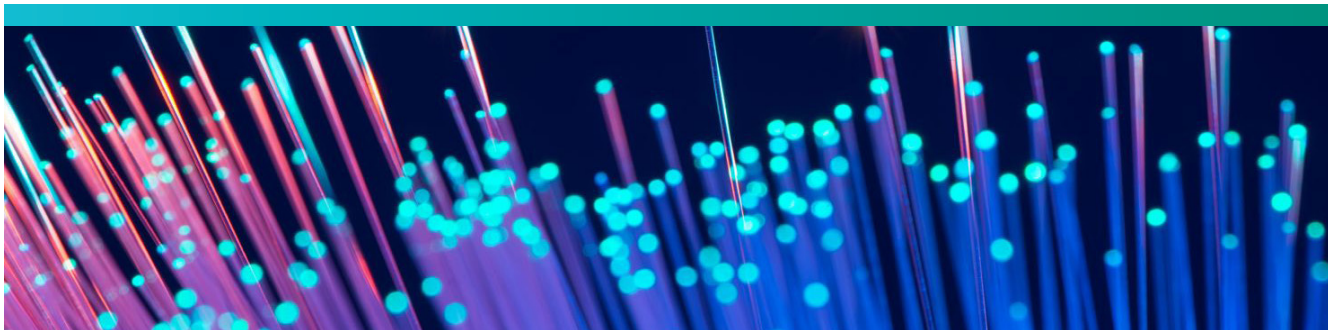
protiviti®
Face the Future with Confidence



Multiple-level Protection Scheme

In part one of our Point of View (POV) series *Interpretations of the updates to China's Cybersecurity Law*, we highlighted the updated legal requirements that impact organizations looking to do business in mainland China. One of these is the Multi-Level Protection Scheme (MLPS), an administrative requirement found in Article 21 of the Cybersecurity Law. Initially introduced in 1994, an updated MLPS 2.0 was issued in 2019, requiring network operators to ensure their networks are protected against interference, damage, or unauthorized access.

To support the implementation of MLPS 2.0, the National Standardization Management Committee of People's Republic of China published a revised Baseline for Multi-Level Protection of Cybersecurity (GB/T 22239-2019) on 10 May 2019 with an effective date of 1 December 2019.

Under MLPS 2.0, network operators are required to classify their infrastructure and application systems into five separate protection levels and fulfill protection obligations accordingly.

Multi-Level Protection Scheme 2.0 Compliance Procedure Overview

Initial classification

To begin compliance procedures, network operators must first conduct a self-assessment and propose a defined protection level for their network. According to the *Guideline for MLPS Classification*, companies must determine the protection level of their system or application based on two major considerations: impacted object and impacted level.

Impacted objects refer to who or what will be potentially impacted by network disruption or a cybersecurity incident. These include Chinese citizens, individuals and other organizations, social interest and public order, or national security. Impacted level refers to whether network disruptions or a cybersecurity incident will cause minor, major, or critical levels of impact on the objects.

A network's protection level is graded according to its degree of societal impact within two benchmarks. The first benchmark assesses the importance of the network with regards to national security, economic construction, and social life. The second benchmark assesses the level of harm network disruption or a cybersecurity incident could cause to national security, public order and interest, and the interest and lawful rights of related citizens, legal persons, and other organizations.

As such, networks that do not affect national security, social order, and public interests are usually classified as Level 1, while networks that may affect social order and public interest are classified as Level 2 or above.[1] Systems or applications with higher degrees of impact are more likely to be classified as Level 3 or even Level 4. Level 5 is usually reserved for state-owned military systems.

Registration with local police agency

Currently, systems or applications should be registered for MLPS within 30 days after the protection level is determined. Do note, however, that the Multi-Level Protection Scheme Rules (Drafted for Comment) will eventually decrease the period to 10 days for Level 2 classifications and above. Local police will review the registration and may either approve the registration and officially issue an MLPS Registration Certificate or reject the application and require the applicant to make rectifications accordingly.

Companies must submit multiple compliance documents with their registration. Documents required for each company may differ depending on local rules and regulations. Network operators should check the official websites[2] for confirmation before submission.

Types of required documents for systems and applications of Level 2 classification and above[3]

- Multi-Level Protection Classification Report
- Multi-Level Protection Registration Application Form
- Expert Classification Review Opinion
- Network and Information Security Commitment
- MLPS Emergency Contact Registration Form

Additional required documents for systems and applications of Level 3 classification and above

- System Architecture and Topology Description
- Cyber Security Organization and Management Policy
- System Security and Protection Measures
- Security Product Inventory and Sale Permit
- System Classification Assessment Report
- Regulatory Agency Review and Approval

[1] More information on ranking criteria may be found in OneTrust DataGuidance's article on the Multi-Level Protection Scheme.
[2] The official website for Beijing may be found here, and the official website for Shanghai may be found here.
[3] This is the full list of required documents for Beijing. Other provinces may have different requirements.

Key Requirements for Compliance

Network operators must comply with both general and extended requirements in order to fulfil their legal obligations around multi-level protection. Compliance requirements are defined according to the associated protection level.

General requirements cover technical solutions and security management. Technical solutions include requirements on physical environment, communications network, network border protection, data security protection, and security operations. Security management covers security policy, security organization, security resources, project management, and operations management.

Extended requirements focus on the security requirements of specific types of platforms, including cloud computing, mobile, Internet of Things (IoT), industrial control systems, and big data.

Required additional security review for Level 2 and above

If a network is determined to be Level 2 or above, the network operator must engage a qualified expert to carry out additional security reviews. Qualified experts are usually a third-party agency, but they can also be certified security professionals within the organization. The review process is very similar to other security audits and technical assessments: the qualified expert will interview the IT management and technical staff, as well as security professionals, to understand current security governance and practices. They will also examine the documented security design and related policies and procedures to assess whether appropriate security controls are within the requirements of the specific protection level. A minimum score of 75 is necessary to pass the assessment for MLPS 2.0.

Verification of assessment by government-approved experts

The above assessment results must be evaluated and endorsed by an independent expert recognized by the MLPS regulatory body. The independent expert is required to provide official documents to confirm assessment results.

Government approval

The above security assessment result and verification should be provided as supplementary documents to the branch of the local police agency where the registration was filed. The process of MLPS compliance is completed once the documents are confirmed by the Ministry of Public Security and an official MLPS certification is issued.

Re-evaluation schedule

Regular re-evaluations are required for systems and applications classified as Level 3 and above. The higher the protection level, the more frequently re-assessments should be conducted in order to stay in compliance with MLPS, with Level 2 networks re-assessed every two years, Level 3 networks re-assessed annually, and Level 4 networks re-assessed every six months. For Level 5 networks, re-evaluation will be defined and managed by respective regulatory ministry and commissions.

Compliance Considerations & Challenges

Technology Compatibility and Risk

MLPS compliance depends on the specific protection level of the targeted systems and applications, as well as the requirements of particular industry regulators. It is important to note that a perfect score is not necessary for MPLS compliance, and network operators should not try to implement all the requirements. Not only is it expensive to do so, attempting to fulfill all requirements may cause companies to risk implementing incompatible technologies, especially if they already utilize another standard, such as ISO27001 or NIST. Implementing MPLS for the sake of compliance and without proper analysis and redesign may, in fact, reduce the level of cybersecurity protection.

Companies should also consider the capabilities of its cybersecurity team when implementing certain technologies. For example, technologies such as SELinux, a Linux security module, requires a high level of technical knowledge and the ability to manage superuser privilege. Without the proper capacities, it may be more prudent for a network operator to disable SELinux or other technologies requiring specialized expertise.

Budget Plan and Cost

MPLS compliance is not a one-time action. Network operators should create a budget plan to ensure that they remain in compliance from the time the system goes online until it is retired. When defining the protection level and developing a budget, network operators should consider long-term system compliance expenditures, as well as indirect costs.

Examples of direct and indirect compliance costs:

Direct compliance cost

- MLPS evaluation cost
- MLPS remediation cost
- Product and device purchasing cost

Indirect compliance cost

- Cost of additional security systems and devices
- MLPS consulting and pre-evaluation cost
- Additional resource costs from MLPS compliance
- Additional maintenance or change for affected systems
- Additional services cost from MLPS
- Travel and overtime costs for internal and external staff
- Collateral damage from system malfunctions and business disruption

Protiviti Cybersecurity and Privacy Protection Services

IT Specialized Audit	• Often included in the overall audit co-sourcing or outsourcing program • More in-depth and technical than Information Technology General Control (ITGC) audit • Often focused on a specific part of IT operations such as Cybersecurity or Disaster Recovery
Security Risk and Compliance Assessment	• International Security Standards: ISO/IEC 2700x, NIST Cybersecurity Framework, CSA Cloud Control Matrix • Payment Card Security Standards: PCI DSS 3.x • Other Regulations/Standards: China Cybersecurity Law, HKMA, SFC, MAS, COSO SOX, ISO/IEC 27701
Data Privacy Services	• Compliance assessment against privacy regulations: Hong Kong PDPO Cap.486, China Personal Information Protection, EU GDPR, US CCPA • Managed privacy services: Privacy-as-a-service • Personal data inventory advisory
Attack and Penetration Service	• Vulnerability scan and penetration test • Source code review • Red team test • Phishing and social engineering test
Security Program and Strategy Design	• Design and revision of cybersecurity strategy and program • Design and revision of security policies, such as data and information classification • Design, revision, and implementation of security procedures
Security Architecture and Control Design	• System hardening review and enhancement • Security architecture design: on-premise, cloud platform • Security control design and review: firewall, data loss prevention, privileged access management, event log analyzer
Security Implementation Services	• Security tools design and selection • Project management and support for security tools implementation • Leverage Protiviti global partnerships with OneTrust, SailPoint, CyberArk, Palo Alto, ServiceNow, Carbon Black, Splunk, LogRhythm, etc.
Managed Security Services	• Security resource augmentation • Managed security operations • Third-party risk outsourcing
Incident Response and Forensics	• Security incident response advisory and support • Security incident investigation and root-cause analysis • Compromise assessment
Security Awareness and Capability Advisory	• Blueteam security assessment and advisory (e.g. SOC, MSSP) • Cyber incident handling and mitigation review • Security awareness assessment and support

How Protiviti Can Help

Protiviti helps businesses in ensuring that their IT services meet legal requirements and regulatory rules on both national and industry-specific levels. With a team of IT security professionals, compliance experts, auditors, and other professionals, Protiviti keeps track of evolving regulations based on industry innovations, environmental trends, and emerging risks.

Protiviti will evaluate your current compliance status and recommend technical solutions to increase the return of investment on MLPS while limiting any impact on your IT and business operations. Our compliance experts will monitor the published technical standards and provide professional opinions on MLPS compliance to help your enterprise continuously meet national standards and requirements.

Contacts

Beijing

Unit 718, China World Office 1
No. 1 Jianguomenwai Street
Chaoyang District
Beijing 100004, China
Tel: (86.10) 8515 1233

Shanghai

Rm. 1915-16, Bldg. 2, International Commerce Centre
No. 288 South Shaanxi Road
Xuhui District
Shanghai 200030, China
Tel: (86.21) 5153 6900

ShenZhen

Unit 1404, Tower One, Kerry Plaza
No. 1 Zhong Xin Si Road
Futian District
Shenzhen 518048, China
Tel: (86.755) 2598 2086

HongKong

9th Floor, Nexxus Building
41 Connaught Road
Central, Hong Kong
Tel: (852) 2238 0499