Cybersecurity Policy Update on MLPS 2.0 and CIIOs

25 September 2020

Sinolytics GmbH | www.sinolytics.de | info@sinolytics.de

sinolytics

New policy officially implements MLPS grading system and CIIO responsibilities

- *"Guiding Opinions"* on Multi-level Protection Scheme (MLPS 2.0) and Critical Information Infrastructure Operators (CIIO), **published 22nd Sep, 2020 and effective 1st Nov, 2020**
- **The "Opinions"** officially launch the MLPS 2.0 and CIIO regulatory frameworks as part of the implementation process of China's Cyber Security Law

Cybersecurity Law Rules

- Multi-level Protection Scheme (MLPS) 2.0 requires entities that operate information networks in China to grade their security level and comply with relevant requirements
- Critical Information Infrastructure Operators operate "key" network systems (e.g. energy) and face extra cybersecurity scrutiny

Current "Guiding Opinions"

《贯彻落实网络安全等级保护制度和关键信息基础设施安全保护制度的指导意见》

"Guiding Opinions on Implementing the Multi-Level Protection System for Network Security and Critical Information Infrastructure Security Protection System"

Issuer: Ministry of Public Security

	Key Facts	Key Implications for Companies
MLPS 2.0	• Network operators must carry out grading work for network systems, according to classification standard GB/T 22240-2020, • Network operators must comply with cybersecurity requirements according to standard GB/T 22239-2020,	• Network operators must conduct a self-assessment • Lv2 or above information networks must file with local PSB and do regular testing evaluations (等级评级) • Lv3 or above information networks have to conduct reporting and testing evaluations once a year and face extra requirements (e.g. risk assessment of service providers, increased encryption requirements)
CIIOs	• Ministry of Public Security is responsible for CIIO top-level design • Industry regulators (finance, energy, defense, etc.) shall define and supervise CIIOs • CIIOs shall set up dedicated cybersecurity units to undertake protection tasks	• Potential CIIOs have to conduct an assessment according to industry regulation • CIIO face extra protection requirements (e.g. CIIOs should store all important and personal data in China) • Network product suppliers of CIIOs face extra security assessment and tightened procurement rules
Work coordination	• Industry authorities, network operators, and public security agencies shall coordinate to carry out security monitoring, early warning systems, emergency response etc. to improve the ability to respond to and deal with cybersecurity emergencies	• Lv3+ companies should build a notification mechanism with industry authorities to strengthen early warning capabilities in their industry • CIIOs, network operators, and public security agencies must build network security monitoring and command centers and implement a 7×24-hour on-duty system

sinolytics

MLPS: All firms operating networks have to follow MLPS 2.0 requirements

MLPS 2.0 sets rules for all companies that operate networks ("network operators") to increase **security protection capabilities**, including the ability to prevent threats, detect security incidents and recover after damage

Companies need to grade their MLPS 2.0 level…

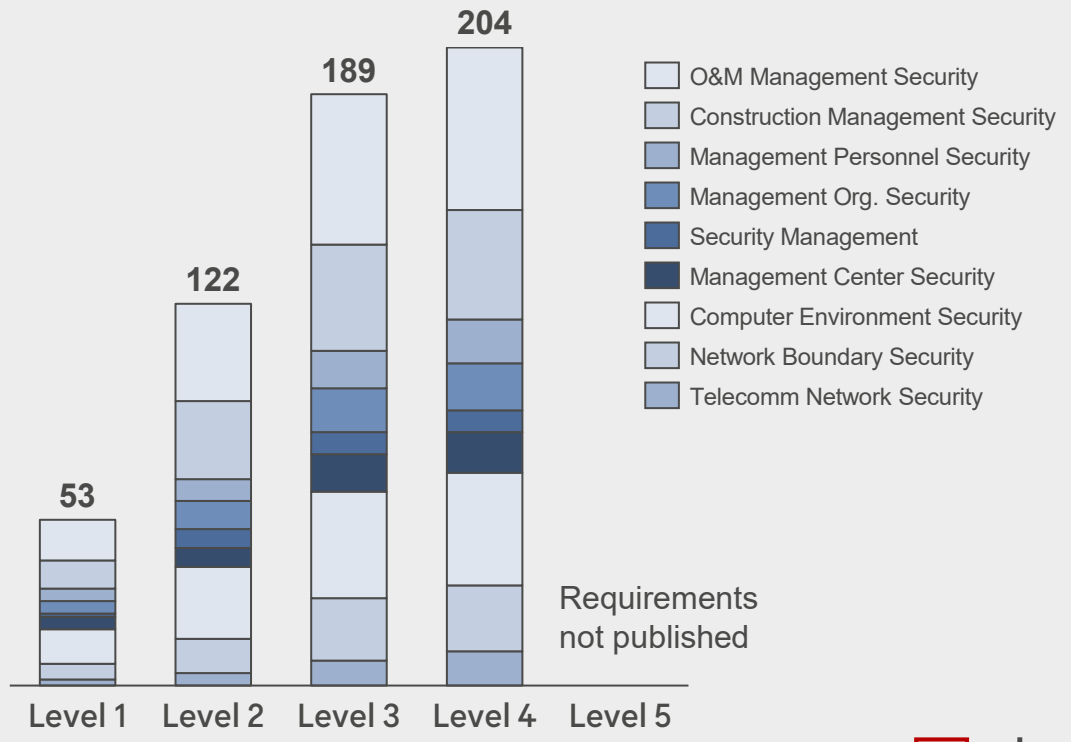
- Network operators are obligated to conduct a self-assessment
- Above level 2 are subject to extra expert evaluation
- Above level 2 need to file with local public security bureaus

Level Grading depends on the potential damage a cybersecurity incident can create for various objects:

	Level 1	Level 2	Level 3	Level 4	Level 5
Legal rights of civilians and legal persons	Damage	Serious Damage	Very Serious Damage		
		OR	OR		
Public order and benefit		Damage	Serious Damage	Very Serious Damage	
			OR	OR	
Nat'l Security			Damage	Serious Damage	Very Serious Damage

…and comply with corresponding requirements

- The number of technical requirements in various security areas increase for higher MLPS 2.0 levels



Source: Cybersecurity standards and Sinolytics research

sinolytics

CIIO: Critical Information Infrastructure Operators face extensive requirements

- Regulations for Critical Information Infrastructure Operators (CIIOs) will be defined by sector regulators according to sector criteria
- Possibly affected companies have to prepare for a level of high scrutiny

Actual CIIOs will be defined by sector regulators

- Cybersecurity Law provides a general definition: CIIOs may **gravely harm national security, the national economy, the people's livelihood and the public interest** once sabotaged
- It is likely that any company categorized above Level 3 of the MLPS 2.0 will be a CIIO

…based on official and draft guidelines companies in following industries can be CIIOS

Financial	• Bank operators • Securities and futures trading • Insurance
Telecomm.	• Data center/cloud services • Voice, data, internet network and hubs
Health	• Health institutions such as hospitals • Disease control • Emergency centers
Production	• Intelligent manufacturing system • Operation and control of high-risk industrial facilities
Water conservancy	• Long-distance water delivery • Urban water source • Water conservancy hub
City infrastructure	• Sewage treatment • Urban rail transit • Smart City operation & mgmt

Companies that are CIIOs face further cybersecurity requirements (examples)

Asset risk assessment: CIIOs have to conduct a **risk assessment of all assets** (incl. data, facilities) towards public/national security in case of data breach

Data storage: CIIOs have to store important and sensitive personal information in **separate data servers**

Supply chain: All **network providers and servicers** to CIIOs have to undergo cybersecurity review procurement procedures and a security risk report

Post-incident recovery: Post-cyber incident recovery requires instant back-up system