CHECKLIST

NETWORK SECURITY LAW OF CHINA

LATHAM&WATKINS

Are you on track for compliance with Network Security Law of China?

This checklist of the Network Security Law of China ("**NSL**") summarizes the key requirements and highlights the most important actions required by the NSL that took effect on 1 June 2017. This checklist is not meant to be exhaustive or exclusive as there are pre-NSL rules and regulations as well as NSL implemental rules and regulations that might be applicable to your company.

As the NSL sets out different requirements based on the regulated parties, this Checklist sets out three sections applicable to each of such parties: (i) owners and administrators of networks and network service providers in China ("**Network Operators**"); (ii) operators of critical information infrastructure ("**CIIO**")[1]; and (iii) manufacturers or suppliers of network related products or services in China.

The requirements introduced in the NSL are wide reaching, and some of these requirements will create profound implications to a number of functions within your organization.

Your Chinese Contacts

Hui Xu
Partner, Shanghai
T +86.21.6101.6006
E hui.xu@lw.com

Lex Kuo
Counsel, Beijing
T +86.10.5965.7043
E lex.kuo@lw.com

Linda Zheng
Associate, Beijing
T +86.10.5965.7027
E linda.zheng@lw.com

Your Global Contacts

Gail Crawford
Partner, London
T +44.20.7710.3001
E gail.crawford@lw.com

Jennifer Archie
Partner, Washington, D.C.
T +1.202.637.2205
E jennifer.archie@lw.com

Serrin Turner
Partner, New York
T +1.212.906.1330
E serrin.turner@lw.com

[1] While NSL provides a broad description of the term "critical information infrastructure" (the "**CII**"), the definition of CII is still pending clarifications by State Council. The CII is broadly described under NSL to cover infrastructure used by the public communications and information services, energy, transportation, water conservancy, finance, public utilities and e-government affairs sectors, and any other infrastructure that, if damaged or malfunctioning, could significantly jeopardize the PRC's national security or public interests.

Category	Action(s) / Deliverable(s)	NSL Article(s)
1. Requirements applicable to Network Operators		
Governance: Personnel and Infrastructure	☐ Monitor updates regarding the NSL, and implement relevant measures accordingly – for instance, the relevant requirement applicable to your organization will be based on your organization's Network Security Classification, which is still pending further clarifications from the relevant authorities.	21
	☐ Introduce external facing terms of services, policies, guidelines, and/or directions ("**Policies and Guidelines**") or review your existing Policies and Guidelines and make amendments to ensure compliance of relevant requirements under the NSL.	21(1)
	☐ Introduce internal Network Security Governance Model and relevant Operation Guidelines or review existing internal Policies and Guidelines and make adjustments to ensure compliance of relevant requirements.	21(1)
	☐ Designate specific personnel to manage network security matters and set out clear functions, roles, responsibilities and reporting lines for such personnel.	21(1)
	☐ Ensure each key network security management and supervising personnel will maintain confidential the personal information, privacy information, and trade secrets they can access when performing their duties (e.g., when entering into confidentiality agreements).	45
	☐ Adopt technologies and establish infrastructure that is sufficient to prevent, alert, and record network security hazards, such as viruses, cyber-attacks, and network intrusions ("**Network Security Hazards**").	21(2)
	☐ Establish and publicize information about channels for accepting complaints or reports about issues regarding network data security issues (e.g., personal information protection).	49
Operation Security	☐ Implement measures to monitor network operations and network security related activities.	21(3)
	☐ Introduce emergency plans or review exiting plans in order to effectively and timely respond to system loopholes and Network Security Hazards.	25
	☐ Implement measures to identify any products or services that are specifically used for intruding networks, interfering network operations or security measures, or stealing network data.	27
	☐ Review Policies and Guidelines as well as contracts to ensure that your organization will be allowed to suspend any network services if you become aware that your services are used for activities that will endanger network security.	27
	☐ Ensure the network product and service procured and used receives regular updating.	22

Category	Action(s) / Deliverable(s)	NSL Article(s)
Data Management	☐ Ensure the keeping of records of at least six (6) months of logs regarding network operations and network security related activities.	21(3)
	☐ Ensure your system supports data classification[2], data back-up and data encryption.	21(4)
Content Management	☐ Establish and implement internal procedures to review your external communications regarding Network Security Hazards to ensure that they are compliant with relevant regulations.	26
	☐ Review the information available on your network and identify prohibited or restricted information, such as information that: (i) endangers national security or interferes economy or social order; (ii) infringes rights or interests of others (e.g., privacy); or (iii) damages physical or mental health of minors.	12, 13
	☐ Implement procedures and measures that could promptly identify and take-down information available on your network in connection with: (i) committing fraud; (ii) imparting methods for committing crimes; (iii) producing or selling prohibited, restricted or controlled merchandise or substance; or (iv) any other illegal criminal activities.	46
	☐ Ensure procedures and measures are in place to manage, identify, take down and erase user-submitted materials containing information that is restricted or prohibited from distribution, and to take measures to prevent further dissemination of such restricted or prohibited information.	47
	☐ Implement procedures and measures to manage, identify, take down and erase emails or applications that contain malicious software or prohibited/restricted information.	48
	☐ Ensure procedures and measures are in place to keep relevant records relating to the restricted or prohibited information or malice software, and to report such incidents to the relevant authorities.	47, 48
	☐ Implement procedures and measures to promptly suspend services provided to the users that: (i) publish or disseminate restricted or prohibited information; or (ii) circulate or distribute emails/applications containing malice software or restricted or prohibited information.	47, 48
Procurement Management	☐ Incorporate procedures to verify compliance of network products and/or services, if procured, with requisite government requirements (see Trial Measures on Security Review of Network Product and Service).	22
	☐ Incorporate procedures to verify certificate of network critical equipment and network security product, if procured, with the state mandatory standards.	23

[2] The NSL does not clarify the "data classification (数据分类)" requirements, and it is expected to be further clarified by the relevant authorities.

Category	Action(s) / Deliverable(s)	NSL Article(s)
	☐ Ensure procurement process has controls to ensure privacy by design (e.g., security diligence, data minimization, visibility of onwards data flows).	42
	☐ Conduct periodic audit of suppliers of network products and services to ensure compliance of such products and/or services.	22
User Identity Verification	☐ Implement identity management and authentication solutions.	24
	☐ Implement measures to verify users identity before providing them with access to your network services, including access to services of internet, landline or cell phone, URL registrations, and services of online content publishing or instant messaging.	24
User Consent and Privacy Policy	☐ Expressly notify users and obtain informed consent from users prior to collecting, processing, sharing and transferring personal information (provided that transferring anonymized personal information does not require consent from users).	41, 42
	☐ Review existing grounds for lawful collecting and processing personal information, and confirm that these will still be sufficient under the NSL (e.g., under NSL, a Network Operator can only collect personal information that is strictly necessary in respect of a particular business purpose and must delete such information as soon as the purpose is achieved).	41
	☐ Where consent is relied upon as the ground for processing personal information, review existing consents to ensure they still meet the NSL requirements.	41
	☐ Introduce NSL-compliant privacy policy or review existing one and make requisite amendments to ensure the privacy policy complies with the NSL. Under the NSL, a privacy policy should set out rules for collecting and using personal information and should specify purposes, means and scopes of data collection and usage.	41
	☐ Ensure technical and operational processes are in place to ensure data subjects' rights can be met, including the right to delete or correct personal information collected by Network Operators.	43
	☐ Ensure the supplier of network product and service receives express consent from users if the used network product and service has such a feature.	
Data Breach	☐ Adopt technologies, establish infrastructure, and take measures that are sufficient to prevent leakage, falsification, damage or loss of personal information.	42
	☐ Stipulate emergency plans of remedial measures for leakage, damage and loss of personal information.	42
	☐ Incorporate procedures to notify users and report to government authorities in case of leakage, damage and loss of personal information.	42

Category	Action(s) / Deliverable(s)	NSL Article(s)
	☐ Review insurance coverage for data breaches and consider whether it needs to be updated.	
Compliant Contract	☐ Develop contract wording for customer agreements and third party vendor agreements that is complaint with the NSL. ☐ Identify all contracts that require relevant contract wording, prioritize and develop process for amending.	
Government Interactions	☐ Establish standard operation procedures and designate relevant personnel for government interactions, which may include, among others: ☐ (i) providing information as required by government authorities: ☐ (ii) granting technical support or assistance: ☐ (iii) accepting government inspections or interview appointments with your organization's key personnel: ☐ (iv) analyzing and evaluating information regarding network security risks: or ☐ (iv) taking technical measures or other necessary measures to eliminate potential security risks and to prevent aggravation of such risks.	28, 49, 54, 55
2. Additional Requirements Applicable to CIIOs		
Governance: Personnel and Infrastructure	☐ Set up a designated security management working committee with proper authority. ☐ Appoint designated security management in-charge personnel and conduct background check of the in-charge personnel and other personnel holding key positions. ☐ Adopt technologies and establish infrastructure that can support stable and continuous business operations, and ensure security measures be designed, established and implemented simultaneously with such infrastructure.	34(1) 34 (1) 33
Security Management	☐ Stipulate new emergency plans for network security matters or review existing plans, and conduct periodic drills. ☐ Stipulate standard procedures to accommodate government authorities' requests for periodic drills of network emergency plans.	34 (4) 39 (2)
Network Products and	☐ Ensure critical network equipment and/or network security products[3] to be procured by a CIIO are certified or inspected by qualified certification organization.	23

[3] The relevant government authority will publish a catalog of critical network equipment and network security products.

Category	Action(s) / Deliverable(s)	NSL Article(s)
Services	☐ Ensure proper procedures are in place to clear national security review on procurement by CIIOs of network products and/or services that could potentially affect national security.	35
	☐ Enter into confidentiality agreement with CIIOs' suppliers of network products and/or services.	36
Data Management	☐ Implement disaster back-up copy of material system and database.	34(3)
	☐ Review existing data storage arrangements for personal data and critical information collected by CIIOs ("**CIIO Critical Data**") during operations within China, and implement necessary changes to ensure local storage of the CIIO Critical Data.	37
	☐ Review existing data access arrangements for the CIIO Critical Data, incorporate control mechanism for accessing the CIIO Critical Data, and implement procedures to clear security assessment before any outbound transmission of the CIIO Critical Data.	37
Trainings, Inspection and Evaluation	☐ Conduct periodic network security trainings and technical trainings for employees and other relevant personnel.	34 (2)
	☐ Undergo at least one inspection/evaluation annually of CIIOs' network security and potential risks ("**CIIO Annual Inspection**") by CIIOs or external qualified network security service provider(s).	38
	☐ Implement procedures to ensure results and reports for improvements of the CIIO Annual Inspection. CIIO Annual Inspection to be submitted to CIIO's department that oversees network security matters.	38
	☐ Stipulate standard procedures to accommodate government authorities' inspection requests and improvement suggestions.	39 (1)
3. Separate Requirements Applicable to Providers of Network Services or Products		
Certification and Quality Control	☐ Verify whether network products and/or services comply with mandatory national standards.	22
	☐ Ensure critical network equipment and network security products are certified or inspected by a qualified certification organization before entering into market.	23
	☐ Implement quality control procedures to ensure the network products and/or services do not contain malicious software.	22
	☐ Ensure procedures are in place to provide remedial measures and notifications to users and government authorities when security defects or loopholes in the network products and/or services are identified.	22
	☐ Ensure continuous security support for network products and/or services for the period required by law or pursuant to user agreements.	22

Category	Action(s) / Deliverable(s)	NSL Article(s)
	☐ Expressly notify users and obtain users' consent before collecting users' information from network products and/or services.	22
	☐ Review contracts to ensure capability to suspend network products and/or services if you become aware that such products and/or services are used for activities that endanger network security.	27

Beijing
Unit 2318
China World Trade Office 2
1 Jian Guo Men Wai Avenue
Beijing 100004
People's Republic of China
t: +86.10.5965.7000

Hong Kong
18th Floor
One Exchange Square
8 Connaught Place, Central
Hong Kong
t: +852.2912.2500

Shanghai
26th Floor, Two ifc
8 Century Boulevard
Shanghai 200120
People's Republic of China
t: +86.21.6101.6000

London
99 Bishopsgate
London
EC2M 3XF
United Kingdom
t: +44(0)20.7710.1000

New York
885 Third Avenue
New York, New York
10022-4834
United States
t: +1.212.906.1200

Washington, D.C.
555 Eleventh Street, NW
Suite 1000
Washington, District of Columbia
20004-1304
United States
t: +1.202.637.2200