China moves to implement security review of network products and services: but leaves foreign investor and manufacturer concerns unanswered

February 2017

Hogan Lovells

China moves to implement security review of network products and services: but leaves foreign investor and manufacturer concerns unanswered

Overview and background

On 4 February 2017, the Cyberspace Administration of China ("**CAC**") issued a draft of the Network Products and Services Security Review Measures ("**Draft Measures**") for public comment: the Draft Measures remain open for comments until 4 March 2017. The Draft Measures are follow-on legislation to China's Cyber Security Law (see our briefings **here**) adopted on 7 November 2016, which will take effect from 1 June 2017 (the "**Cyber Security Law**").

The Draft Measures bring China one step closer to implementing a security review regime with respect to network products and services (and their providers), a process first set in motion by the Cyber Security Law. How this regime would look was one of several major areas of concern for foreign investors arising out of the implementation of the Cyber Security Law in China. Given the recent direction China has taken in this regard, and a previous campaign to introduce the "secure and controllable"[1] concept in the banking, securities and insurance sectors, there were legitimate concerns that a new program of security review might be skewed in favour of "local" manufacturers and thus become a back door means of imposing essentially protectionist policies. In the case of the previous "secure and controllable" campaign, in some sectors, even though the campaign was eventually suspended, some such protectionist effects were felt, as it seemed that some businesses in China may have taken the view in light of impending requirements that buying local products was a better, lower risk purchasing strategy than buying products manufactured overseas or by foreign-invested enterprises ("**FIEs**") in China, so these concerns are quite real.

The background to the Draft Measures is that the Cyber Security Law requires that network products and services purchased by operators of "critical information infrastructure" (the definition of which is somewhat vague and unsatisfactory, see our previous analysis **here**) ("**CIOs**") must undergo national security review ("**Security Review**") if such network products and services "might potentially have an impact on national security", failing which the CIO risks being ordered to discontinue use and/or being subject to quite stiff fines (up to ten times the purchase price) and, in a formulation reminiscent of the *PRC Criminal Law*, the persons directly in charge and other directly responsible persons will be liable to pay personal fines between RMB 10,000 and 100,000.

Thus, since the promulgation of the Cyber Security Law (which has yet to come into force), it has been known that a Security Review regime would be introduced for certain network products and services, potentially impacting both the businesses who are manufacturers of such products and providers of such services as well as the users (or prospective users) of those products and services. The Draft Measures aim to give shape to such Security Review, but as drafted leave a number of critical questions unanswered.

Do the draft measures answer all the questions?

The Draft Measures fill in some of the details of the Security Review process, primarily by setting forth the broad content areas to be covered and by establishing its bureaucratic framework.

---

1 Sometimes formulated as "secure and reliable".

2 The Cyber Security Law also requires a security certification or security testing regime for "key network equipment" and "specialized products for network security" (see Article 23 of the Cyber Security Law). However, the Draft Measures apparently do not address these requirements. Note that this Security Review also appears to be completely separate to the process for obtaining a Network Access Permit ("**NAP**") under the *Telecom Equipment Network Access Administrative Procedures* amended with effect from 23 September 2014 (the "**NAP Measures**") which already applies to most network and terminal equipment. Where required, a NAP must be obtained before connecting certain networking and terminal equipment such as mobile telephones or routers to a network in China.

However, the Draft Measures do little to settle some of the key areas of uncertainty that have arisen around the Security Review process, including:

— More precision around which products and services might be viewed as having an impact on national security and therefore potentially subject to Security Review;

— More precision around which companies are considered to be CIOs and therefore potentially limited in their procurement options; and

— Whether there will be a protectionist slant in the Security Reviews, such that their practical implementation will make it difficult for foreign or FIE manufacturers to compete.

Perhaps the biggest concern is that, even if passed in their current form, the Draft Measures also do not set out the specific standards and procedures applicable to Security Review. On an optimistic view, the Draft Measures should only be an intermediate step closer to the launch of the Security Review regime, not the final step, and more legislation (perhaps in the form of further CAC implementing rules) should follow, bringing clarity. A more cynical view is that certain obvious gaps will persist in any event, and in practice will simply be filled in by opaque, subjective interpretation.

The Draft Measures also introduce some new potential areas of "scope creep" for rules that on their face are meant to be directed at cyber security concerns. For example (and as explained in more detail below), Security Reviews are to include an assessment of the risk that users could become so reliant on a technology that it gives rise to unfair competition, which is not a risk that would ordinarily be seen as part of a technology risk management exercise (and is a concern already addressed under other Chinese laws).

Scope of application

Article 2 of the Draft Measures provides that "important network products and services used by information systems which concern national security and the public interest are subject to network security review". Article 2 thus sets out an opaque and potentially broad scope of application for Security Review. However, it is the restrictions on procurement set out in the Draft Measures which really illustrate the "consequences" for failing to achieve certification:

— **Party and government authorities** and **key industries** must purchase network products and services which have passed Security Review on a priority basis, while refraining from purchasing any network products and services which have failed to pass Security Review.

— **CIOs** may only purchase network products and services which have passed network security review if such network products and services may have an impact on national security (as determined by the government departments in charge of protecting the security of critical information infrastructure).

The second bullet point above is consistent with the text of the Cyber Security Law, but like the Cyber Security Law carries with it some uncertainty as to the scope of its application, as "critical information infrastructure" has yet to be fully defined (see our discussion on this **here**). The first bullet point above, by contrast, goes even further than the requirements under the Cyber Security Law and introduces further uncertainty, as the term "key industries" is not exhaustively defined but clearly allows the scope for sectors forced to buy only certified products and services to be expanded, based on subjective interpretation of what is a "key sector" going beyond those listed.

The foregoing provisions on procurement might suggest limited impact for product and service providers whose target markets do not include party and government authorities, key industries,

and CIOs in segments touching upon national security. Absent any amendment or clarification to the Draft Measures, however, we do not expect a limited impact, given that "key industries" and "operators of critical information infrastructure" may be interpreted to apply to a broad swath of companies, and given the likelihood that some companies e.g. state-owned enterprises outside these defined categories may also voluntarily chose to (or come under pressure to) give priority to purchasing products that have passed Security Review and are readily available on commercial terms. The teeth in the imposition of the "secure and controllable" policy in the banking sector was not so much the threat of punishment for violating the legislation, but more in the commercial pressure brought to bear in the tendering and procurement of equipment processes by State-owned banks, where in practice any bidder that failed to meet the given "secure and controllable" criteria would essentially find its bid marked down to the point where the bid was virtually or literally disqualified.

What does Security Review involve?

The Draft Measures implicitly require that network products and services be "secure" and "controllable", and in this regard require the assessment of the following potential risks:

- The risk that such products or services might be subject to unlawful control, interference or operational shutdowns;
- Risks occurring during the course of research, development, delivery and technical support in relation to the products and key components thereof;
- The risk that the product or service provider might be able to use the provision of such product or service as a means to unlawfully collect, store, process or use related user information;
- The risk that the product or service provider might be able to take advantage of users' reliance on such product or service to engage in unfair competition or activities detrimental to user interests; and
- Other risks which may jeopardize national security or harm the public interest.

The first bullet point seems to be taking aim at whether the products are at risk of being hacked, infected by viruses, and/or controlled or turned off remotely.

The second bullet point is more oblique and likely contemplates a number of risks, some of which relate to the broad concerns set out in the first bullet. Risks concerning the development of the products and its components points would include software "back doors", "logic bombs" and other code that would have been deliberately installed as part of the development with a view to allowing data extraction or remote operation. It could also involve an assessment of how secure the course of development of the technology was and, for example, assessing the risk that knowledge of the security features of the technology such as encryption/decryption keys has "leaked" or has otherwise become known outside the developer's organization, or that software or firmware, whether open source or sourced from a third party, has not been properly screened prior to its use in the product. Risks concerning technical support of a product could point to the product's reliance on remote support, whether within or outside of China, or to the customer's access to source code, and so may be a further point of concern about the Security Review for foreign technology providers in particular.

The third bullet point takes aim at data protection concerns around user information, in particular the risk that products collect and process information without the user's knowledge. Unlike in the

first bullet point, the focus here is on misconduct by product and service providers and not third parties that may hack into the product.

The fourth bullet point seems to be something of a mixed concept, whereby it hints at issues like abuse of a dominant market position with the words "might be able to take advantage of users reliance on such product or service to engage in unfair competition" but also brings up more generalized and vague notions of the provider or manufacturer engaging in behavior prejudicial to users which points to consumer protection-type laws. The risk highlighted here is not one which would ordinarily be seen as a direct concern from a network security perspective.

What is interesting or you could say unfortunate about this, is how China appears to have conflated what some might argue are non-national security-related issues like data protection and acts of unfair competition in what is supposed to be a national security test. These areas are already extensively addressed in other parts of Chinese law, so it is difficult to see why they should form part of a national security test.

The unfair competition/prejudicial conduct to users part is not just vague, it is also largely subjective and could be used to fail a product manufactured overseas or by an FIE for the wrong reasons: any service or product provider regardless of origin has the potential for abusing its position as vendor or supplier in a manner that goes against the interests of the consumer, depending on how you define "abuse", so the question becomes how do you make an objective, non-political decision whether or not to pass based on the potential for abuse?

As for the sweep up at the end: as drafted, this is basically a purely subjective test of anything else that may have been omitted from the legislation or which may be determined as harming the public interest as determined by the CAC or the institutions or experts making the determination. It is so broad as to make the other criteria basically redundant, as virtually anything could be fitted within this category.

Security review process framework

The Draft Measures set out a multi-layered, multi-institutional approach to Security Review, which we have illustrated in chart form in the Appendix.

The top layer is the CAC, which will promulgate the legislation in its final form and will be responsible for its interpretation.

The next layer down is a Network Security Review Committee ("**NSR Committee**"). The NSR Committee will be established by the CAC, together with other departments in charge (perhaps the Ministry of Industry and Information Technology ("**MIIT**") and/or others), and will be responsible for deliberating on major Security Review policies, uniformly organizing network security review efforts, and coordinating major Security Review issues.

The next layer down is a Network Security Review Office ("**NSR Office**"). Though not specifically defined, the NSR Office might presumably be a local office under the CAC. Each NSR Office is in charge of the specific organization and implementation of Security Reviews.

The NSR Office will arrange for two other groups of actors – (1) third-party institutions and (2) experts – to actually conduct Security Reviews, where and as required based on the requirements of the State, the advice of national trade associations, market reactions, applications by enterprises and so forth. One of the dangers of such broadly consultative approach is how the NSR Office will balance comments or recommendations and, for example, filter out those driven by protectionist motives.

Third-party institution review apparently comes first. Such third-party institutions are to be designated by an as-yet unspecified organ of the state (so are not independent in any sense) and clearly there is a risk of decisions being driven by undue influence. The third-party institution will

conduct a third-party evaluation. After that, a committee of experts (formed by the NSR Committee), taking the third-party evaluation as a basis, will conduct an overall assessment of (1) the security risks of a given network product or service, as well as (2) the security and reliability of the provider of such product or services. In a partial nod to greater transparency, security review results will be then published by the NSR Office "within a defined scope", so presumably with the parts relating to national security redacted.

Government authorities in "key industries" such as finance, telecommunications, energy and so forth (and therefore potentially others) are responsible for Security Reviews in their respective industries and sectors. It is not entirely clear, though, whether involvement of sector-specific authorities in Security Reviews puts those reviews on a separate track from other industries, or whether their participation is an additional layer, and how products and services that are used across multiple industries will be treated.

This does not augur well for overseas or FIE manufacturers who may, in the industry-organised reviews, come up against some of the government and regulatory bodies that historically have been less open to foreign investment. Many of the officials in those bodies and/or in the ranks of review institutions or experts will have worked in, or spent time with domestic players (those who have worked overseas or for FIEs or overseas manufacturers are likely to be in the minority) who will be seeking Security Review for their products, leading to obvious conflicts of interest. Other risks are exactly the same as those that have plagued invitation to tender bid panels in China: manufacturers and other interested parties will try to pre-determine the outcome by identifying and seeking to influence the members of the group who make the final decision. Article 12 alludes to this risk by requiring these third party institutions to conduct an "objective, impartial and fair evaluation of the product, services and the provider", but this is really only a counsel of perfection and the potential for gaming the system through undue influence is undeniable. Article 13 alludes to another major issue: how to ensure the reviewers do not disclose confidential information revealed during the review process. This is discussed in detail below.

Security of proprietary information

Article 13 makes the position of the equipment or service provider with respect to compliance abundantly clear when it says: "Network product and service providers must cooperate with network security reviews." These will undoubtedly include disclosure of certain product/service information, some of which may be sensitive and/or proprietary and constitute valuable intellectual property rights ("**IPR**"). This raises concerns about the security of such disclosed information and potential theft or loss of IPR as a pre-condition to gaining market access.

The Draft Measures attempt to provide some comfort in this regard by providing that third party institutions and other relevant entities and personnel (e.g. experts) are obligated to maintain the security and confidentiality of any information to which they have access during the course of a security review, and must not use such information for purposes other than performing network security review.

However, we expect this will provide little real comfort, as no punishments are specified for the contravention of these measures and leaks and misappropriation can be virtually impossible to trace; obtaining adequate redress in the Chinese courts may not be realistic or achievable in the absence of overwhelming evidence. Understandably, some multi-national companies providing network products and services may prefer to only provide non-front-line or a limited range of products in China to mitigate the risk of disclosures of "crown jewels" IPR. And, of course, the "elephant in the room" (on which the Draft Measures are predictably silent) is whether passing certification means disclosing source code in part or in whole. Given the fact that the Draft Measures potentially allow and essentially require a wide range of government and Party bodies and other key industry participants to shun non-certified products, the commercial pressure on

those overseas or FIE manufacturers who service those markets and industries to obtain certification is likely to be intense if they want to continue to service those markets; hence the pressure to produce source code once a request is made is also likely to be intense, bearing in mind, as noted above, that "cooperation" is mandatory.

Conclusion

National security is by definition a rather murky area of law and so it could not have realistically been expected that the Draft Measures would bring laser-like precision to the new Security Review process.

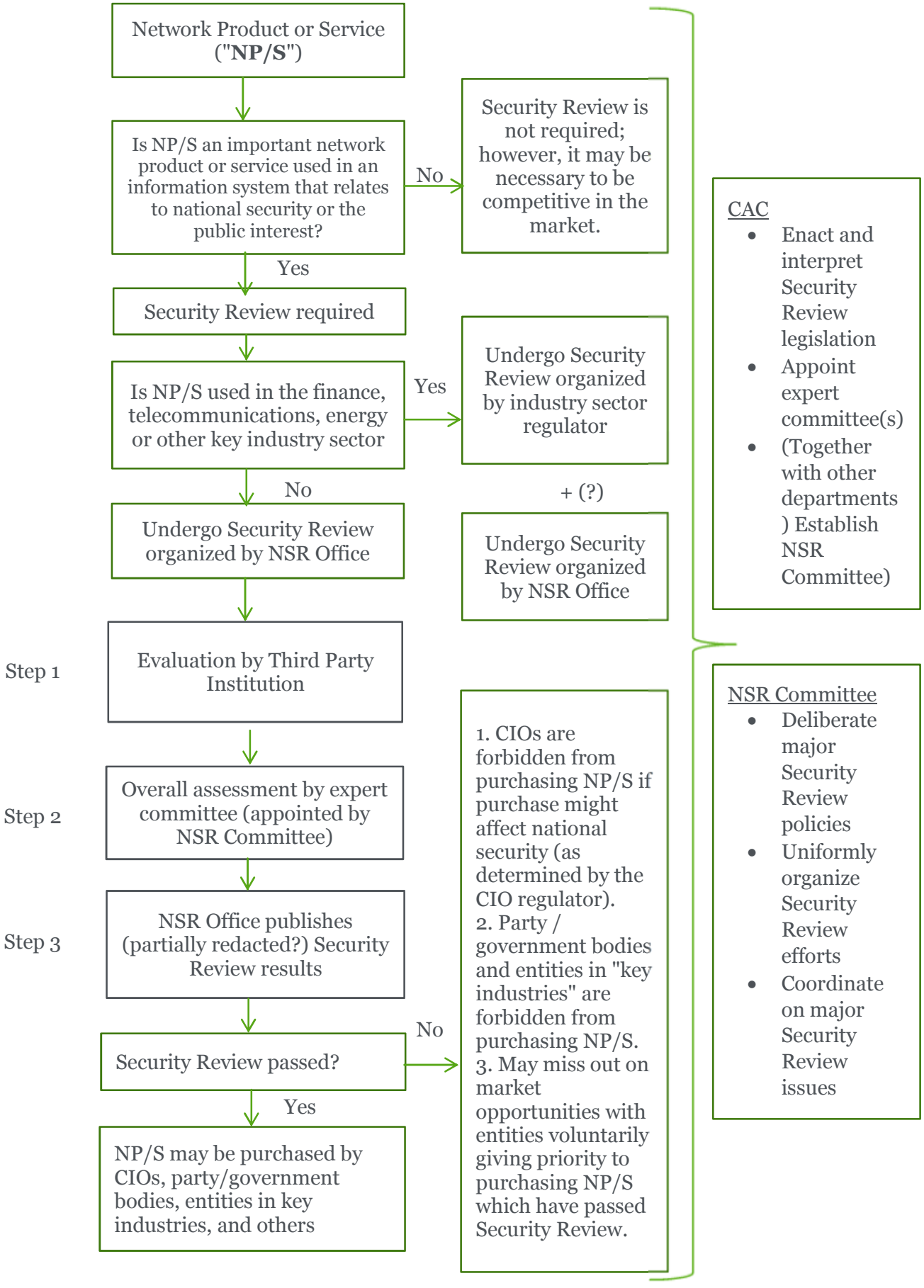
However even the minimalist expectations of the foreign investor/manufacturer community are likely to have been disappointed by the Draft Measures, which suffer from the following obvious and essential flaws, to name but a few:

- No further clarity on which products and services are subject to Security Review: essentially an unsatisfactory and ultimately subjective test of: "Important network products and services used by information systems which concern national security and the public interest" will determine this;
- No further clarity on which companies will be considered CIOs;
- A national security review test that conflates areas already addressed elsewhere in Chinese law and which do not obviously belong in the national security review context;
- A multi-layer government-driven bureaucracy organizes the review process and chooses all the participants with no safeguards on independence built in at any stage;
- No obvious filtering mechanisms to prevent protectionist data and recommendations being put forward by trade associations or market players;
- No clear machinery to prevent government officials with conflicts of interest (e.g. ties to industry participants whose equipment or services is under review) from participating in the review process;
- Many industries which have historically tended to be most closed to foreign investment will organize and carry out their own sector-based review processes;
- No definitive list of the "key industries" which will be under an obligation to purchase certified equipment and services, so the list can be extended based on subjective interpretation;
- No provision imposing accountability or specific punishments on participants who fail to conduct an "objective, impartial and fair evaluation" other than "being held responsible for the results of their evaluations";
- No mention of whether source code can be requested, but an obligation to cooperate means that if requested, network product and service providers have an obligation to provide it;
- No safeguards built in to prevent corruption in the process or gaming the system through undue influence (although arguably partially covered by existing legislation); and
- No mention of any review or appeal procedure for an interested party who feels the outcome of a Security Review was seriously flawed.

All in all, the Draft Measures do little to address or alleviate foreign investor or manufacturer concerns that came out of the passing of the Cyber Security Law in relation to Security Review. At most the Security Review process is now a little clearer. All that can be hoped for is that subsequent drafts can address at least some of the key issues raised above.

Please continue to the next page to see our Appendix showing the Security Review process in chart form.

Appendix – Security Review Process Tree



Contacts

Andrew McGinty
Partner, Shanghai
andrew.mcginty@hoganlovells.com

Philip Cheng
Partner, Shanghai
philip.cheng@hoganlovells.com

Liang Xu
Partner, Beijing
liang.xu@hoganlovells.com

Mark Parsons
Partner, Hong Kong
mark.parsons@hoganlovells.com

Nolan Shaw
Associate, Beijing
nolan.shaw@hoganlovells.com

Alicante
Amsterdam
Baltimore
Beijing
Brussels
Budapest
Caracas
Colorado Springs
Denver
Dubai
Dusseldorf
Frankfurt
Hamburg
Hanoi
Ho Chi Minh City
Hong Kong
Houston
Jakarta
Johannesburg
London
Los Angeles
Louisville
Luxembourg
Madrid
Mexico City
Miami
Milan
Minneapolis
Monterrey
Moscow
Munich
New York
Northern Virginia
Paris
Perth
Philadelphia
Rio de Janeiro
Rome
San Francisco
São Paulo
Shanghai
Shanghai FTZ
Silicon Valley
Singapore
Sydney
Tokyo
Ulaanbaatar
Warsaw
Washington, D.C.
Zagreb

Our offices
Associated offices

www.hoganlovells.com