SHIN&KIM
법무법인(유) 세종

Proposed Amendments to the Network Act: Key Trends and Implications

2026.05.07

Following a series of recent high profile security breach incidents, there is growing consensus on the need to strengthen the overall legal framework governing such matters. Against this background, amendments to the *Act on Promotion of Information and Communications Network Utilization and Information Protection* (the "**Network Act**")—which include provisions to enhance the accountability of Chief Information Security Officers (CISOs), establish Information Security Committees, reinforce the Information Security Management System (ISMS) certification regime, and impose penalty surcharges for repeated incidents—have recently passed the National Assembly and now face being enforced. *
** For further details, please refer to our firm's newsletter dated March 19, 2026.* [Link]

In addition, several additional bills proposing amendments to the Network Act are currently pending before the Science, ICT, Broadcasting and Communications Committee of the National Assembly. These bills seek to reinforce the liability of the information and communications service provider ("service provider") for security incidents, while also establishing an institutional framework to foster 'white-hat hackers.' Notably, some of these bills were referred to the Third Legislative Review Subcommittee on Information, Communications, Broadcasting and Media ("**Subcommittee**") on April 21, 2026, and are currently under deliberation.

The following provides an overview of the key provisions of the Network Act amendment bills referred to the Subcommittee, with a particular focus on the bill proposed by Assembly Member Lee Haimin, together with their key implications.

1. Key Provisions of the Proposed Amendments

▶ Bill Proposed by Assembly Member Lee Haimin

The bill proposed by Assembly Member Lee Haimin (Bill No. 2215361, introduced on December 18, 2025) is grounded in the recognition that there is an urgent need to establish an effective response framework for security breach incidents. The principal features of the bill include:

(i) requiring service providers to bear the full costs of operating a joint public private investigation team (the "**Joint Investigation Team**") where a security breach incident is attributable to the service provider;
(ii) shifting the burden of proof in damages claims such that the service provider must demonstrate the absence of intent or negligence; and
(iii) introducing a punitive damages regime.

1) Liability for Investigation Costs – Article 48-4(9)

Under the current Network Act, the Minister of Science and ICT (the "**Minister**") is authorized to establish a private-public joint investigation team in the event of a serious security breach incident, with the full operating costs of such investigation borne by the government.

The proposed amendment introduces a material shift in cost allocation. Where a security breach incident has occurred due to reasons attributable to a service provider, the service provider may be required to bear the full costs incurred in operating the Joint Investigation Team. As a result, in such cases the burden on the service providers is expected to increase.

2) Shift in the Burden of Proof in Damages Claims – Article 48-7(1)

The proposed amendment introduces a new Article 48 7, under which users may claim damages against a service provider where a security breach incident occurs as a result of the service provider's violation of the Network Act and causes harm to users. In such cases, the service provider will not be exempt from liability unless it proves the absence of intent or negligence on its part.

If the proposed amendment is passed, users will only be required to prove that a loss occurred and the burden of proof regarding other elements—specifically causation and the service provider's intent or negligence—will shift to the service provider. Consequently, this is expected to lead to a significant increase in the number of damage claims following security breach incidents.

3) Introduction of Punitive Damages – Article 48-7(2), (3)

Damages for security breach incidents under the current Network Act are limited to the amount of actual loss. The proposed amendment, however, introduces a punitive damages regime. Where a security breach is caused by the intent or gross negligence of a service provider, the court may award damages of up to three times the amount of actual damages.

In determining the amount of punitive damages, the court may take into account factors such as the scale of harm suffered, the duration and frequency of the security breach incidents, and the financial standing of the service provider. Accordingly, if the proposed amendment is passed, service providers with significant annual revenues or those found responsible for repeated or serious security breach incidents are expected to face higher damages being awarded.

▶ Key Provisions of the Amendment Bills Proposed by other Assembly Members

In addition to the bill proposed by Assembly Member Lee Haimin, a number of other proposed amendment bills referred to the Subcommittee also contain provisions addressing security breach incidents. The key features of these proposed amendment bills are summarized below.

- **Inspection of Network Connected Devices**
  To prevent security breach incidents involving information and communications network connected devices ("**Network-Connected Devices**"), the bill seeks to authorize the Minister to conduct inspections of the information security practices of Network Connected Devices with a high risk of security breach incidents, publicly disclose the results of such inspections, and issue recommendations for improvement to manufacturers or importers of the relevant Network-Connected Devices based on the inspection findings (*Bill proposed by Assembly Member Choi Minhee, Bill No. 2215299, introduced on December 16, 2025*).
- **Enhanced Cloud and Supply Chain Management**
  To effectively manage increasingly complex IT supply chains resulting from the adoption of cloud servers and the use of external vendors, the bill aims to specify detailed information security requirements applicable to service providers. These requirements include, among others, account management for remote access users and outsourced service providers, detection of anomalous insider activities, and security measures for cloud environments and IT supply chains. The bill would further mandate the retention of information security audit materials in relation to a security breach incident. In addition, where incidents that materially undermine the safety or reliability of user information have occurred, or are likely to occur, the Minister would be authorized to require the submission of audit and remediation related materials (*Bill proposed by Assembly Member Choi Hyungdu, Bill No. 2216230, introduced on January 22, 2026*).
- **Fostering White-Hat Hackers**
  To legitimize and promote the security activities of private sector security experts, including white hat hackers, for the prevention of security breach incidents, the bill would allow service providers and other relevant entities to establish and publicly disclose vulnerability handling policies. The bill would further provide a legal basis for limiting liability for information security researchers who conduct activities in compliance with such policies, and would mandate government reporting and user notification with respect to critical security vulnerabilities (*Bill proposed by Assembly Member Choi Hyungdu, Bill No. 2216276, introduced on January 23, 2026*).

2. Key Implications

- **Need for Continuous Monitoring of Legislative Developments**
  Recent amendments to the Network Act, as well as to the Personal Information Protection Act ("**PIPA**"), have strengthened service provider accountability in connection with security breach incidents, including through the introduction of penalty surcharges of a punitive nature for repeated or serious violations. In light of these legislative trends, there is a substantial likelihood that many of the proposed amendments discussed above will be reflected, at least in part, in future amendments to the Network Act. Accordingly, service providers should continue to closely monitor developments in the legislative and regulatory landscape.
- **Need for Compliance Review**
  The legal and regulatory framework relating to security breach incidents is evolving in a direction that increases the responsibility of service providers, including the amendments to the Network Act that recently passed the National Assembly. In this context, there is a need for service providers to review and assess their overall compliance with regulatory requirements relating to security breach incidents. To this end, service providers may

consider conducting a comprehensive compliance review in advance, including the preparation of compliance checklists, the revision of internal policies and manuals, and organizational diagnostics.

About Shin & Kim’s ICT Group

Shin & Kim’s ICT Group provides comprehensive, one-stop legal services by leveraging the firm's distinctive expertise and extensive professional network in the ICT sector, having consistently earned the highest client recognition in recent years. Drawing upon our deep-seated capabilities in broadcasting, telecommunications, personal information protection, and internet IT, we deliver the highest level of legal advisory services encompassing regulatory trend analysis in broadcasting, telecommunications, and ICT; government affairs and legislative improvement & consulting; regulatory impact assessment; and corporate strategic planning. Furthermore, we possess extensive experience and exceptional expertise in personal information/AI compliance and risk management, providing holistic analysis and strategic responses to legal issues and regulatory risks associated with AI adoption and deployment across diverse industry sectors. Please feel free to contact us with any questions or if you require our assistance on any ICT-related legal matters.

[Korean version]「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 주요 개정 동향 및 시사점

Key Contacts

Kwang-Hee Choi
Senior Advisor

+82-2-316-4651
khchoi@shinkim.com

Sinook Kang
Senior Partner

+82-2-316-4059
sokang@shinkim.com

Jeong Ho Ahn
Partner

+82-2-316-2891
jhahn@shinkim.com

Jin Hong Noh
Partner

+82-2-316-1639
jhnoh@shinkim.com

Chang Jun Park
Partner

+82-2-316-1660
cjpark@shinkim.com

Sally Lim
Foreign Attorney

+82-2-316-7266
slim@shinkim.com

So Jeong Jeong

Associate

+82-2-316-1877
sjjeong@shinkim.com
