Baker McKenzie.

Dispute Resolution / IP Tech
Tokyo

Client Alert

14 August 2025

Japan's Active Cyber Defense Law: what businesses need to know

For further information please contact:

Kensaku Takase
Partner
+81 3 6271 9752
Kensaku.Takase@bakermckenzie.com

Daisuke Tatsuno
Partner
+81 3 6271 9479
Daisuke.Tatsuno@bakermckenzie.com

Dominic Sharman
Partner
+81 3 6271 9496
dominic.sharman@bakermckenzie.com

To address the growing threat of cyberattacks targeting government systems and critical infrastructure, Japan has enacted the Active Cyber Defense Law[1] ("ACD"). The ACD is a landmark legislative framework that empowers both public and private sectors to proactively defend against cyber threats.

The law was enacted on 16 May 2025 and will take full effect by 2027 by way of a phased implementation.

The ACD has the following four strategic pillars:

1. Strengthening public-private collaboration

   It aims for stronger cooperation between government and private entities, including (i) information sharing and analysis and (ii) coordinated vulnerability response.

2. Use of communication data

   It grants the government authority to collect and analyze communication data under certain conditions to detect and respond to cyber threats.

3. Access and neutralization

   It authorizes the government to access and neutralize attacker infrastructure including servers used for cyberattacks.

4. Organizational and structural readiness

   It establishes new governance structures and protocols to support national cyber defense capabilities.

Of these, pillars 1. and 2. are likely to have the most significant impacts on private businesses.

A. Who is affected?

The following businesses need to comply with the new obligations under the ACD:

i. Critical Infrastructure Operators ("CIOs")

   Entities designated as "Specified Social Infrastructure Providers" under the Economic Security Promotion Act, including business operators that offer

[1] The Active Cyber Defense Law refers to the Act on Prevention of Damage Caused by Unlawful Acts Against Important Electronic Computers ("**Cyber Reinforcement Act**") and the Act on Establishment of Relevant Laws regarding the Enforcement of the Act on Prevention of Damage Caused by Unlawful Acts Against Important Electronic Computers ("**Cyber Establishment Act**").


Yuki Kondo
Senior Associate
+81 3 6271 9765
Yuki.Kondo@bakermckenzie.com


Aya Takahashi
Associate
+81 3 6271 9522
Aya.Takahashi@bakermckenzie.com


Rieko Yamauchi
Associate
+81 3 6271 9890
Rieko.Yamauchi@bakermckenzie.com


Hayato Higa
Associate
+81 3 6271 9519
Hayato.Higa@bakermckenzie.com

essential infrastructure services (such as electricity, gas, telecommunications and finance).

ii. Telecommunications service providers

Telecommunications service providers as defined under the Telecommunications Business Act (including carriers operating key network infrastructure).

iii. IT vendors

Manufacturers, importers, distributors and providers of computers (or programs embedded therein and used as part of Critical Systems).

B. Key obligations for those affected

(i) Critical Infrastructure Operators

- Notification obligations regarding Key Systems

  CIOs must notify regulators when introducing certain important systems ("Critical Systems") that are identified by the relevant regulations as carrying a risk of interrupting or diminishing the functions of facilities and programs used for their infrastructure services (should cybersecurity be compromised).

- Incident reporting obligations

  CIOs are required to report cybersecurity incidents or potential threats involving Critical Systems to both the relevant ministries and the Prime Minister's Office.

- Cooperation on data sharing with authorities

  The government may ask CIOs to enter into an agreement to share cross-border communication data. While executing the agreement is voluntary, CIOs must engage in discussions with the government unless they have a justifiable reason not to. The government will conduct a cybersecurity analysis using data provided by CIOs and share the results with them.

- Establishment of a new council

  To prevent damage from cyberattacks, the Council on Information Sharing and Countermeasures ("Council") will be established. CIOs and IT vendors will be added as Council members once they have given their consent. The Council is authorized to share confidential, security-relevant information with its members and may request the submission of data or other forms of cooperation necessary to prevent cyber-related harm.

(ii) Telecommunications service providers

- Government access to communication data without business's consent

  With the approval of the Cyber Communications Oversight Committee, the government may access communication data when it suspects

cyberattack-related communications have been transmitted. Access will only be allowed when it is difficult to detect and assess cyber-attacks by other means (i.e., foreign-to-foreign communications) or when analyzing communications with designated foreign systems is necessary to detect cyber threats targeting Japan (i.e., foreign-to-domestic and domestic-to-foreign communications).

Telecommunications service providers may be required to cooperate with the government, including by providing information about their facilities and connecting equipment for data sharing. They are not permitted to refuse such a request without a justifiable reason.

(iii) IT vendors

- Vulnerability disclosure and remediation

  The ACD introduces enhanced vulnerability management as part of its public-private collaboration framework.

  The government may notify relevant IT vendors about vulnerabilities identified in Critical Systems and publish remediation guidance. For vulnerabilities affecting Critical Systems, the competent minister may request that corrective actions be taken and reports and information be submitted. While these requests are not binding, vendors will need to make reasonable efforts to respond.

- Cooperation with CIOs

  IT vendors may be indirectly impacted by CIOs' incident reporting obligations. If a vendor is targeted in a cyberattack, the CIOs may request that a vendor cooperate in fulfilling its reporting obligation.

C. What should businesses do now?

- Assess the applicability of the ACD

  Analyze whether your organization is subject to, or affected by, the obligations under the ACD.

- Establish internal rules and reporting processes

  Develop internal protocols for system registration, incident reporting, and responding to government data-sharing or remediation requests.

- Monitor regulatory developments

  Key implementation details will be defined in forthcoming ministerial ordinances. Stay alert for updates and prepare to adapt compliance strategies accordingly.

- Strengthen internal cybersecurity protocols

  Enhance your organization's cybersecurity program to meet heightened expectations and potential obligations under the ACD.

D. Conclusion

The cyber defense space, not unlike the "traditional" defense space, is developing rapidly amid efforts to counter ever-evolving threats. The ACD will come into force against this background with potentially wide-ranging implications for vast swathes of businesses in the private sector. The ACD also presents opportunities for businesses engaged in providing services in the cyber defense arena.

We strongly encourage companies to keep up to date using our Connect on Tech blog or newsletters and reach out to our specialists with any questions on steps they should take in connection with the ACD.