NEWSLETTER

Introduction of a New Security Clearance System —Enactment of the Act on the Protection and Use of Critical Economic Security Information—

Competition Law / International Trade Newsletter June 14, 2024

Authors:
Yuki Sakurada
y.sakurada@nishimura.com
Takayoshi Hojo
ta.hojo@nishimura.com
Kei Ogawa
k.ogawa@nishimura.com
Kazuki Yoshii
k.yoshii@nishimura.com

The Act on the Protection and Use of Critical Economic Security Information (the "**Act**"), which introduces a new security clearance system,[1] was passed through Diet deliberations on May 10, 2024.[2]

The Act is scheduled to come into effect on a date to be specified by a Cabinet Order within a period not exceeding one year from now, and the details of the system are expected to be specified by operational standards and Cabinet Orders to be established in the future. This newsletter explains noteworthy points for companies that may receive information subject to the Act's protection, to the extent available at enactment.

1. Overview of the Act on the Protection and Use of Critical Economic Security Information

(1) Background and Purpose of Enactment

The Act was developed through the "Final Summary Report"[3] published by the "Expert Council on Security Clearance Systems in the Economic Security Field," established on February 21, 2023, after about a year of discussions, and the sixth meeting of the Council for the Promotion of Economic Security held on January 30, 2024,[4] and the bill was submitted to the Diet on February 27, 2024.

Simply stated, the purpose of the Act is to strengthen Japan's information security by only granting persons with

---

1 The security clearance system is described as a system in which, as part of national information security measures, the government conducts an investigation of persons (e.g., government officials and, if necessary, employees of private business operators) who need access to information classified as security-critical (Classified Information; "**CI**") held by the government, and grants access to such persons after confirming their trustworthiness.

2 The House of Representatives passed the revised bill submitted to the Diet after the Cabinet decision, and forwarded it to the House of Councilors (the submitted bill and the revised bill passed by the House of Representatives). For a summary of the revised portions, see (6) below.

3 "Final Summary Report" of the Expert Council on Security Clearance System in the Economic Security Field dated January 19, 2024 (the "**Final Summary Report**").

4 Cabinet Secretariat, "Council for the Promotion of Economic Security (Sixth Meeting)."

certain qualifications access to critical information concerning the economic security of critical infrastructure and critical product supply chains, and to facilitate utilization of such information (see Article 1 of the Act). Although the preceding Act on the Protection of Specially Designated Secrets (Specially Designated Secret Protection Act or "**SDSPA**") already has provisions regarding the security clearance system, the SDSPA limits the specially designated secrets to be protected to information in four fields: defense, diplomacy, prevention of specified harmful activities, and prevention of terrorism. Accordingly, the Act will strengthen information security in the economic security field. The industry also expects that the introduction of a new system based on the Act will "contribute to expanding opportunities for companies to participate in activities such as international joint research and development."[5]

(2) Scope of Information Subject to Preservation under the Act (Act, Article 3)

The information protected under the Act (i.e., that subject to the security clearance system) is defined as "Critical Economic Security Information" ("**CESI**"). Each administrative organ shall designate as CESI any information related to critical infrastructure and supply chains of critical products in connection with the affairs under its jurisdiction ("Critical Economic Infrastructure Protection Information"), which is not publicly available and needs to be specifically kept confidential because its leakage may impede the security of Japan[6] (Act, Article 3, paragraph (1)).

A Critical Economic Infrastructure Protection Information

As stated above, CESI is designated from among "Critical Economic Infrastructure Protection Information," which is information about "critical economic infrastructure" (referring to critical infrastructure and supply chains of critical products)[7] and relates to the following (Act, Article 2, paragraph (4)):

(i) measures to protect critical economic infrastructure from attacks from the outside, or plans or research related thereto;
(ii) vulnerability of critical economic infrastructure, innovative technologies related to critical economic infrastructure, and other critical information regarding critical economic infrastructure related to security;
(iii) information collected from foreign governments or international organizations with respect to the measures described in (i); and
(iv) collection and coordination of the information set forth in (ii) and (iii) above or the capacity thereof.

Examples of "Critical Economic Infrastructure Protection Information" are assumed to be information related to **cyber** (cyber threats and countermeasures), **regulatory enforcement** (considerations and analyses by the authorities in their review processes, etc.), **investigations, analyses, and R&D** (industrial and technological strategies, supply chain vulnerabilities, etc.), and **international cooperation** (concerning international joint

---

5 Japan Business Federation (*Keidanren*), "Early enactment of the bill for the Act on the Protection and Use of Critical Economic Security Information is required." (March 19, 2024). It will be necessary to gain confidence from other countries with similar systems that the new system based on the Act is equivalent to those systems.

6 "Security" in the Act is defined as ensuring the security of the nation and its people against external invasions or other threats (Act, Article 1).

7 Act, Article 2, paragraph (3).

R&D).[8]

B Information Held by Private Business Operators

According to the Final Summary Report, under the security clearance system only government-held information qualifies as CESI; therefore, one assumption is that information that is not yet in the government's possession is unlikely to be unilaterally designated as such.[9]

On the other hand, the Act merely stipulates that CESI shall be designated from among "Critical Economic Infrastructure Protection Information in connection with affairs under the jurisdiction of administrative organs" (Act, Article 3, paragraph (1)), and there is no language limiting this to information held by the government. In this regard, we need to pay close attention to how the Act is implemented, along with the provision stipulating the method of providing CESI (see (3) below).

C Relationship with the SDSPA

As stated above, the security clearance system based on the SDSPA covers four fields: defense, diplomacy, prevention of specified harmful activities, and prevention of terrorism.[10] In this regard, the security clearance system based on the Act does not expand the scope of the SDSPA, but rather is a separate system.[11]

However, the two acts' respective institutional frameworks are similar in many respects, and some information critical for economic security includes information that is conceptually subject to the SDSPA.[12] With regard to the Act, there have been some questions as to whether it was necessary to enact a law separate from the SDSPA, or whether the SDSPA could have been amended. However, in the economic security field, it is increasingly recognized that it is important to have public-private partnerships in which information is not only kept secret within the government, but also shared with and utilized by appropriate private business operators, and the provisions of the Act do a better job reflecting this aspect of "use" of information, especially compared to the SDSPA.[13] As such, the necessity of the Act becomes clear when considering these different purposes. In addition, the Act serves as a CI framework for Confidential level information not covered by the current SDSPA out of three CI classifications (Top Secret, Secret, and Confidential) in information protection

---

8 Final Summary Report 4(1)(i).

9 Final Summary Report 4(1)(ii).

10 Appendix of the SDSPA, Standards to ensure uniform implementation in connection with the designation of specially designated secrets and the recission of the designation as well as the conduct of the security clearance assessment.

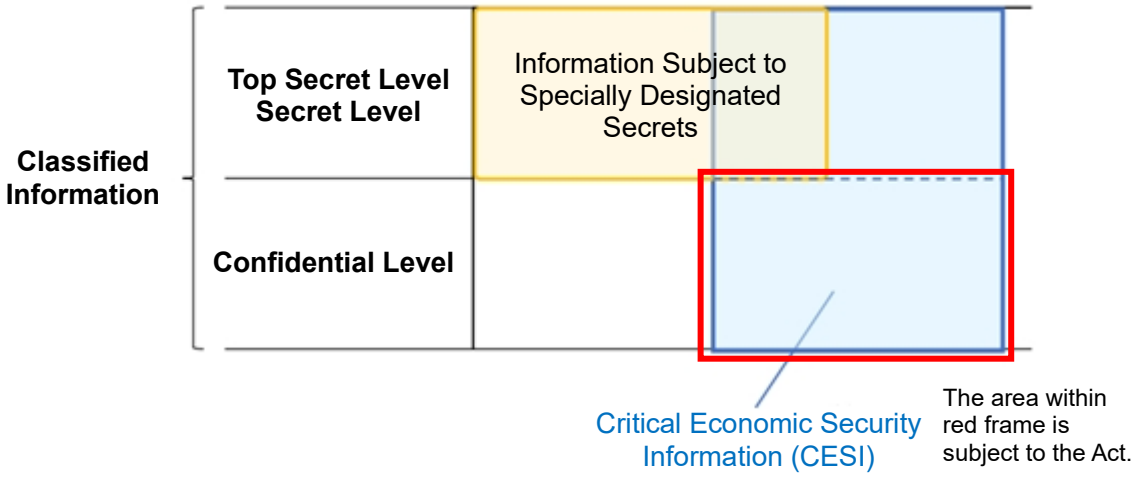
11 The Secretariat's Explanatory Material dated December 20, 2023, prepared by the Cabinet Secretariat, of the Nineth Expert Council on Security Clearance System in the Economic Security Field also states the basic idea that "the SDSPA and the Economic Security Clearance System are two separate systems, and information that falls under the category of specially designated secrets under the SDSPA is not subject to this system" (p. 9).

12 The Secretariat's Explanatory Material dated January 17, 2024, prepared by the Cabinet Secretariat, of the Tenth Expert Council on Security Clearance System in the Economic Security Field lists information that could be critical for economic security, and note that "the above includes information that could fall under the items listed in the Appendix under the SDSPA (p. 3)." In fact, under the Act, CESI is designated excluding specially designated secrets as stipulated in the SDSPA (Act, Article 3, paragraph (1)).

13 The name of the Act is "Act on the Protection ***and Use*** …," and Article 1 of the Act also states that it "provides ... necessary matters concerning the protection ***and Use*** of information." See also minutes of the 213th Diet Session, Cabinet Committee of House of Representatives No. 4 (March 22, 2024), answers and other statements by Minister of State Takaichi.

agreements concluded with other countries; this is a primary difference in the sensitivity of information handled by the Act and that of the SDSPA, which only preserves information designated as "Top Secret" and "Secret."[14] Because of this difference in positioning, there are also differences in the wording, such as specially designated secrets being defined as those whose leakage could ***seriously impede*** the security of Japan [...]" (SDSPA, Article 3, paragraph (1)), while CESI defines them as "those whose leakage could ***impede*** the security of Japan [...]" (Act, Article 3, paragraph (1)).[15]

That being said, the information covered by the Act and the SDSPA are similar (there is some conceptual overlap), and it is necessary to clarify the scope of each law to avoid confusion in practice. Measures are expected to be taken, such as revising the operational standards of the SDSPA and formulating new guidance, to enable seamless operation of both laws.[16]



Source: Prepared by editing materials provided by the Cabinet Secretariat (https://www.cas.go.jp/jp/seisaku/keizai_anzen_hosyo_sc/dai7/siryou.pdf)

D Designation Effective Period

As a general rule, the effective period of the designation of CESI is initially set at up to five years, but may be extended up to a total of 30 years thereafter (Act, Article 4, paragraphs (1) through (3)). However, the effective period may be further extended (beyond the standard 30 years) if the head of an administrative organ obtains approval from the Cabinet that it is unavoidable not to make information subject to the designation public (Act, Article 4, paragraph (4)).

---

14 Final Summary Report 4(1)(i). At the Council for the Promotion of Economic Security (Sixth Meeting), Prime Minister Kishida stated, "In order to protect and use CESI held by the government, a new law will establish a system for the protection of Confidential level information. It is clarified that this is a system for the protection of Confidential level information, not Top Secret or Secret level information.

15 Explanatory Material for the Bill published by the Cabinet Secretariat (Bill for the Act on the Protection and Use of Critical Economic Security Information), p. 2.

16 Prime Minister Kishida has announced his policy that he will take necessary measures to ensure that the Act operates seamlessly with the existing information security system, including consideration whether it is necessary to review the operational standards of the SDSPA (Summary of the 6th Economic Security Promotion Council Meeting).

(3) Provision of CESI to Contractors (Act, Article 10)

Administrative organs provide CESI based on "contracts" with contractors when they find it necessary in order to facilitate activities that contribute to ensuring national security, such as the elimination of vulnerabilities in critical economic infrastructure (Act, Article 10, paragraph (1)). The recipients of the information are limited to certain contractors (eligible contractors) who have indicated their willingness to receive designated information sharing from the government and whose facilities and organizations have been confirmed as qualified.[17]

Since the contract is based on an agreement between the government and the contractor, it is acceptable for the contractor to decide not to enter into the contract and not receive CESI. The standards for facilities and organizations to qualify as eligible contractors (clearance conditions for contractors) will be specified in a Cabinet Order in the future, but similar to the Enforcement Order of the SDSPA, it is assumed that the contractor will establish internal rules regarding the implementation of measures, such as restrictions on entering places where CESI is handled, restrictions on bringing equipment into those places, and training for employees regarding the protection of CESI, and will be recognized to properly protect information by taking measures in accordance with the rules.[18] The Final Summary Report states that an effective and realistic system should be developed based on the operation of the current system (the SDSPA) and examples from major countries, while taking into account the actual situation of companies and consistency with the domestic legal system.[19] In particular, the supplementary resolution to the bill for the Act states that the development of a management system for "Foreign Ownership, Control, or Influence" should be considered and appropriate measures should be taken,[20] and that there is a possibility that the standards for eligible contractors to be established in the future will include, for example, provisions that take into account the influence of foreign shareholders on contractors.[21]

The contract to be concluded with the eligible contractor shall provide for the following matters in accordance with the Act (Act, Article 10, paragraph (3)):[22]

---

17 Article 10, paragraph (2) of the Act provides that if the head of an administrative organ designates as CESI information that it does not hold and that is expected to be held by an eligible contractor through investigations, research, etc., conducted by the eligible contractor under the direction of (with the consent of) the head of the administrative organ, the head of the administrative organ shall notify the eligible contractor who is considered to need to utilize the information of the fact that the information has been designated as such. In this case, the head of the administrative organ may have the information held as CESI based on the contract with the eligible contractor.

18 See the Statement by Mr. Shinagawa, Government Witness in minutes of the 213th Diet Session, Cabinet Committee No. 4 (March 22, 2024). The Final Summary Report 4(2)(iii) indicated the direction to confirm not only physical management requirements such as facilities owned by private business operators, etc., but also organizational requirements such as composition of shareholders and directors of the private business operators, etc.

19 Final Summary Report 4(2)(iii)

20 Supplementary Resolution to the Bill for the Protection and Use of Critical Economic Security Information

21 Final Summary Report 4(2)(iii) mentions the U.S. National Industrial Security Program and its operating manual and notes that there are provisions governing "Foreign Ownership, Control, or Influence" (it also mentions the existence of regulations regarding cybersecurity).

22 See also Explanatory Material for the Bill published by the Cabinet Secretariat (Bill for the Act on the Protection and Use of Critical Economic Security Information), p. 4. It is expected that the government will release a contract template. The Ministry of Defense has published its contract template regarding the provision of specially designated secrets under the SDSPA.

(i) scope of employees nominated by the eligible contractor to handle CESI;
(ii) matters regarding the nomination of a person to manage operations related to the protection of CESI;
(iii) matters regarding the establishment of facilities and equipment necessary for the protection of CESI;
(iv) matters regarding training of employees on the protection of CESI;
(v) statement that CESI must be provided to the head of an administrative organ if requested by the head of the administrative organ; and
(vi) matters specified by Cabinet Order as necessary for the protection of CESI by eligible contractors.

An eligible contractor that receives CESI must take necessary measures to properly protect it and have its employees handle it in accordance with the contract it has concluded (Act, Article 10, paragraph (4)). The scope of these employees is stipulated in the contract (see (i) above). It is assumed that an eligible contractor that has concluded a contract will submit a list of subject employees, after obtaining their consent, to an administrative organ, and then the administrative organ will conduct eligibility assessments of the subject employees (see (4) below).[23]

(4) Assessment of Contractor Employees and Items Examined (Act, Article 11)

Only persons who have passed a security clearance assessment (an assessment to determine whether a potential handler of CESI is likely to leak it, the results of which are valid for ten years) may handle CESI (Act, Article 11, paragraph (1)). However, persons deemed unlikely to be at risk of leaking CESI in a SDSPA eligibility assessment may handle CESI for a period of five years (i.e., the period during which the SDSPA eligibility assessment is valid) without undergoing another security clearance assessment under the Act (Act, Article 11, paragraph (2)).

Security clearance assessments must be performed by the head of an administrative organ, based on the results of a survey of established matters (security clearance assessment survey) after obtaining the consent of the person subject to assessment (Act, Article 12, paragraphs (2) and (3)). However, in principle, the head of the administrative organ shall request that the Prime Minister perform the security clearance assessment survey, and, as a result, **the Security Clearance Assessment Survey is performed by the Prime Minister (Cabinet Office) on a centralized basis** (Act, Article 12, paragraphs (4) and (5)).[24] The Prime Minister shall notify the heads of administrative organs of the results of the security clearance assessment surveys and of the Prime Minister's opinion on the possibility of CESI leaks, in accordance with the Cabinet Order (Act, Article 12, paragraph (5)).[25]

Security clearance assessment surveys are performed on the basis of items (i) through (vii) below (Act,

[23] Explanatory Material for the Bill published by the Cabinet Secretariat (Bill for the Act on the Protection and Use of Critical Economic Security Information), p. 17.

[24] An eligible contractor is required to undergo a security clearance assessment by each administrative organ with which the eligible contractor executes an agreement.

[25] In addition, a person who has undergone a centralized survey by the Prime Minister within ten years, and who has been found to have no risk of leaking CESI when handling CESI, via a security clearance assessment, will not be required to undergo another security clearance assessment survey, because that person will undergo a security clearance assessment based on the results of the centralized survey by the Prime Minister, even if there is a change to the administrative organ that performs the security clearance assessment (Act, Article 12, paragraph (7)).

Article 12, paragraph (2)). The survey items essentially are identical to the items surveyed in an SDSPA security clearance assessment (i.e., referencing the following table, under the SDPSA, items (ii) through (vii) are identical, while item (i) is matters related to the relationship with "specified harmful activities").

Items Surveyed in a Security Clearance Assessment
(i) Matters related to relationships with activities that damage critical economic infrastructure
(ii) Matters related to criminal and disciplinary history
(iii) Matters related to history of non-compliance in handling information
(iv) Matters related to drug abuse and effects
(v) Matters related to mental illness
(vi) Matters related to moderation in alcohol consumption
(vii) Matters related to credit status and other economic conditions

The "activities that damage critical economic infrastructure" in (i) means the following two types of activities:

(a) activities to obtain information that is not publicly known concerning critical economic infrastructure, the leakage of which is likely to impede the security of Japan or other activities, which are conducted for the purpose of benefiting a foreign country and significantly harm or are likely to harm the security of Japan or its citizens with respect to critical economic infrastructure; and

(b) activities designed to cause hindrance to critical economic infrastructure conducted, based on political or other principles, with the purpose of inducing the nation or other persons to conform to such principles, or to create unrest or fear in society.

"Matters related to relationships with activities that damage critical economic infrastructure" (item (i) above) shall include the name, date of birth, nationality, and address of family members and persons living together of persons subject to assessment (Act, Article 12, paragraph (2), item (i)). Therefore, information including the nationality of the person subject to assessment and their family members may be taken into account.[26] Regarding specific survey methods, the explanatory material for the Cabinet Secretariat bill explains that it "assumes checking submitted questionnaires, checking through personnel management information, interviewing the persons subject to assessment themselves and questioning their superiors, and making inquiries to public and private organizations."[27]

(5) Penalties for Leakage of Information

If a person engaged in the handling of CESI leaks CESI that comes to the person's knowledge in the course of the person's duties, the person shall be punished by imprisonment for not more than five years or a fine of not

[26] In a questioning at the House of Representatives Cabinet Committee, Minister Takaichi explained that "the fact that a person subject to security clearance assessment is a foreign national is a factor to be considered as a matter related to relationships with activities that damage critical economic infrastructure under item (i) of the same paragraph" (213th Diet Session, Committee on Cabinet (April 3, 2024)).

[27] Explanatory Material for the Bill published by the Cabinet Secretariat (Bill for the Act on the Protection and Use of Critical Economic Security Information), p. 17.

more than five million yen, or both (Act, Article 23, paragraph (1)). Attempted and negligent violations also are punishable (Act, Article 23, paragraphs (3) and (4)). In addition, there is a dual punishment provision for corporations (i.e., if a representative or employee of a corporation commits a violation in connection with the business of the corporation, not only the violating person shall be punished, but also the corporation shall be fined) (Act, Article 28).

The SDSPA provides for imprisonment for not more than ten years or a combination of imprisonment and a fine of not more than ten million yen for the leakage of specially designated secrets (SDSPA, Article 18, paragraph (1)). The penalties under the Act were determined based on the penalty provisions of the SDSPA and other Acts, taking into consideration the level of secrecy (whether "Top Secret/Secret" level or "Confidential" level) of the information to be protected under the relevant Act.[28]

(6) Institutional Guarantees for Proper Operation of the System (Act, Articles 18 and 19)

In order to properly operate the system, the government is to establish standards for uniform operation with respect to (i) designation and rescission of CESI, (ii) implementation of security clearance assessment, and (iii) certification of eligible contractors (Act, Article 18, paragraph (1)). Such standards are to be formulated after hearing the opinions of experts and are required to be approved by the Cabinet (Act, Article 18, paragraph (2)).

In addition, the Prime Minister must report annually to experts on the status of (i) through (iii) and hear their opinions (Act, Article 18, paragraph (3)), and the government is to report annually to the Diet on the status of (i) through (iii) with the opinions of those experts and make a public announcement (Act, Article 19). The provisions stipulating these reporting and announcement obligations of the government were not included in the initial bill submitted to the House of Representatives, but were added when the bill was amended and passed by the House of Representatives.[29] The Constitutional Democratic Party of Japan, which requested the amendments, explained that the amendments were made to "significantly strengthen oversight by the Diet and within government departments in order to prevent arbitrary operations and black boxing by the government."[30]

(7) Date of Enforcement

The Act will come into force as from the date specified by a Cabinet Order within a period not exceeding one year from the date of promulgation (Act, Supplementary Provisions, Article 1. However, the provisions concerning preparation of and cabinet decision on draft standards for uniform operation (Act, Article 18, paragraphs (i) and (ii)) will come into force as of the day of promulgation).

From now on, until the enforcement of the Act, a Cabinet Order concerning specific operations of the Act will be established. The following are the main items that are specified in the Act as being delegated to a Cabinet

---

28 Final Summary Report, p. 9; 213th Diet Session, House of Representatives, Committee on Cabinet, No. 4 (March 22, 2024), Statement by Mr. Shinagawa, Government Witness

29 Draft Amendments to the Draft Act Concerning the Protection and Use of CESI (LDP, CDP, Nippon Ishin FEFA, Komeito, DPFP, and volunteers)

30 Constitutional Democratic Party of Japan, "[Lower House Plenary Session] House of Representatives member Mr. Honjo pointed out issues in the two economic security bills, including establishment of security clearances" (April 9, 2024).

Order. In addition, matters other than those listed below (e.g., matters concerning procedures and interpretation) also may be indicated by a Cabinet Order:

- standards for certification of eligible contractors (Act, Article 10, paragraph (1));
- matters to be stipulated in an agreement with an eligible contractor (matters to be added to those already stipulated in the Act, Article 10, paragraph (3), items (i) through (v)); and
- specific methods of implementing security clearance assessments and security clearance assessment surveys (Act, Article 12, paragraphs (3) through (5)).

In addition to a Cabinet Order, as mentioned above, operational standards are expected to be established to ensure uniform operation with regard to (i) designation and rescission of Critical Economic Security Information, (ii) implementation of security clearance assessment, and (iii) certification of eligible contractors. Furthermore, the supplementary resolutions of the committee deliberations of the House of Representatives and the House of Councilors provide that certain matters need to be considered (e.g., "specification of prohibited matters in operational standards to ensure effectiveness of unintended-use prohibition provisions" on the results of the security clearance assessments; "guidelines for proper communication, including labor-management consultation" concerning prevention of disadvantageous treatment of workers; and "preparation and public announcement of standards for facility development" for eligible contractors), and these matters will also be specified in the operational standards or some other guidelines that will be prepared separately.

2. Conclusion

As described above, the types of CESI subject to protection under the Act may encompass information related to **cyber** (cyber threats and countermeasures), **regulatory enforcement** (considerations and analyses by the authorities in their review process, etc.), **investigations, analyses, and R&D** (industrial and technological strategies, supply chain vulnerabilities, etc.), and **international cooperation** (international joint R&D). Companies that are expected to obtain those types of information from administrative organs need to consider the following matters in order to be prepared for the enforcement of the Act: (i) fulfillment of facility and organizational requirements to be eligible as an "eligible contractor;" and (ii) handling of officers and employees who are candidates for security clearance assessment.

With respect to (i) above, for meeting facility requirements, the following measures may be considered: restrictions on entry and bringing of equipment into places where CESI is handled; promoting internal awareness of rules and regulations through education on CESI protection; and developing facilities and systems to block access to CESI by persons without clearance. In addition, if Foreign Ownership, Control or Influence (FOCI) is considered as a part of organizational requirements, it may be necessary to take measures to eliminate or reduce foreign shareholder influence.

With regard to formulation of internal rules for employees subject to security clearance assessment and the treatment of those employees, in (ii) above, it may be necessary to consider labor-related laws and regulations as well as the impact on human resources and recruitment. Particular matters that require consideration include methods for identifying departments and employees that may be subject to security clearance assessment, measures to prevent those assessed from being treated disadvantageously (when those assessed do not give consent for security clearance assessment or those assessed cannot obtain clearance), and

methods for managing security clearance assessment results and treatment of persons who obtained clearance.

There are many matters that are not clear at this point, such as specific types of information to be designated as CESI, the extent and number of cases involving such designated CESI by each administrative organ,[31] the facility and organizational requirements to be eligible as a "eligible contractor," and specific terms and types of agreements to be executed by administrative organs.[32] These issues may require us to wait for release of Cabinet Orders and operational standards that are expected to be formulated in the future; however, companies can proceed with preparation with the information that is already available.[33]

Public Relations Section, Nishimura & Asahi newsletter@nishimura.com

31 For reference, with regard to specifically designated secrets, the number of specially designated secrets designated by administrative organs during the year 2022 was 44 (including 25 by the Ministry of Defense and 6 by the Cabinet Secretariat), and the total number of cases where eligibility assessment was conducted was 23,583 (including 19,857 by the Ministry of Defense), of which 22,429 were administrative organ employees or persons in other similar positions and 1,154 were eligible contractor employees. In addition, as of the last day of 2022, the total number of persons who can perform duties of handling specifically designated secrets was 132,567, of which 3,828 were eligible contractor employees (Cabinet Secretariat, June 2023, "Report on Designation and Rescission of Specifically Designated Secrets, and the Implementation Status of Security Clearance Assessment"). In the government's response to a question during deliberation of the Act in the Diet, the government estimated that, (although based on a bold assumption,) in the first year, the number of CESI designation cases would be several dozens or at most three digits, and that the number of persons subject to security clearance assessment would be several thousands, not tens of thousands, per year (Answer by Ms. Takaichi, Minister of State at the joint council of 213th Diet Session, House of Councilors Cabinet Committee and the Committee on Economy, Trade and Industry (April 25, 2024); Answer by the government witness Mr. Iida at the same Cabinet Committee (April 25, 2024), etc.).

32 Examples of assumed situations in which CESI is provided include: provision of information on threats such as cyber attacks on infrastructures and details of the government's countermeasures to infrastructure business operators; provision of information on supply chain vulnerabilities of certain critical goods and external actions targeting them to business operators handling such goods; and provision of information from foreign governments on joint research and development of innovative technologies to business operators participating in such research and development (joint council of 213th Diet Session, House of Councilors Cabinet Committee and the Committee on Economy, Trade and Industry (April 25, 2024)).

33 Reference may be made to the operational status of the SDSPA and the operational status of the Acquisition, Technology & Logistics Agency, which is already requiring management for cases where "Confidential"-level information is provided.