NISHIMURA & ASAHI

西村あさひ法律事務所

Formulation of a New National Security Strategy, Economic Security, and Cybersecurity

Competition Law / International Trade Newsletter January 13, 2023

Authors:
E-mail Yuki Sakurada
E-mail Masahiro Heike
E-mail Taku Nemoto

* This newsletter was drafted based upon the information available as of December 26, 2022.

On December 17, 2022, a new "National Security Strategy of Japan,"[1] "National Defense Strategy," and "Defense Program" (the "National Security Strategy of Japan" is hereinafter referred to as the "**Security Strategy**," and collectively with the National Defense Strategy and Defense Program, the "**Three Security Documents**") were decided by the National Security Council and approved by a Cabinet Decision.

Of these, the Security Strategy is positioned as the supreme national security policy document, and is intended to provide strategic guidance for Japan's national security policy areas, including diplomacy, defense, economic security, technology, cyber, maritime, space, intelligence, official development assistance (ODA), and energy ("I. Purpose" in the Security Strategy). In addition, the National Defense Strategy was formulated to comprehensively present Japan's defense objectives, approaches, and means by which to accomplish those objectives, replacing the National Defense Program Guidelines, which have served as Japan's basic guidelines for development, sustainment, and operation of defense capability with the Self-Defense Forces as its core ("I. Objectives of National Defense Strategy" in the National Defense Strategy). The Defense Program is a program for fundamentally reinforcing Japan's defense capabilities in order to develop Japan's defense capabilities in relation to dealing with invasions of Japan, and disrupting and defeating such threats while obtaining the support of its allies and others by FY2027.[2]

---

1 https://www.mod.go.jp/j/approach/agenda/guideline/pdf/security_strategy_en.pdf

The Security Strategy was formulated for the first time on December 17, 2013 (decided by the National Security Council and approved by a Cabinet Decision on December 17, 2013), and it has been revised for the first time in 9 years.

2 "Opinion on the Formulation of a New National Security Strategy, etc." by the Security Research Committee, Policy Research Council of the Liberal Democratic Party of Japan dated April 26, 2022 (the "**LDP Opinion Dated April 26**") states that since the current National Security Strategy and National Defense Program Guidelines have many overlapping factors in relation to security, the National Security Strategy should focus on specifying the security environment, and national security goals and methods of achieving them at the strategic level, while the National Defense Program Guidelines should formulate a document that focuses on a threat-opposing defense strategy. It further states that a new "National Defense Strategy" that is consistent with the U.S. strategic document system should be formulated, replacing the National Defense Program Guidelines, and that as a document replacing the description of the specific structure of the Japan Self-Defense Forces in the current National Defense Program Guidelines and the current Medium-Term Defense Program, a "Defense Program" for reinforcing national defense capabilities should be formulated ("What the Three Documents Should Be", in the same opinion).

The Three Security Documents stipulate various matters related to security, with a focus on reinforcing the defense system of Japan. Among the matters stipulated in the Three Security Documents, this newsletter attempts to provide a timely commentary on the points that should be noted from the perspectives of economic security and cybersecurity, which may affect the economic activities of companies.[3] Unless otherwise noted, the items cited below in this newsletter refer to the items in the Security Strategy.

(Reference) Table of Contents of the Security Strategy

1. Points to Note From an Economic Security Perspective

- "Economic security" is defined in the Security Strategy, and specifically, it is clarified that "economic

[3] Although omitted from this newsletter due to space limitations, the National Defense Strategy and the Defense Program include various measures to strengthen production bases of the defense industry, such as by enhancing the defense industry supply chain and cybersecurity, and measures to strengthen the defense technology base, such as through the establishment of new research institutes through the scrap-and-build of the research and development organizations of the Acquisition, Technology & Logistics Agency.

In regard to transfers of defense equipment and technology, the Security Strategy and the National Defense Strategy state that reviews of systems, including the Three Principles on Transfer of Defense Equipment and Technology and its Implementation Guidelines, are to be considered in order to smoothly conduct transfers of defense equipment and technology and international joint development having high security significance in a wide variety of fields, and in doing so, ensuring that the necessity, requirements, and transparency of related procedures for transfers of defense equipment and technology will be adequately considered, while maintaining the three principles themselves. In addition, the National Defense Strategy and the Defense Program include measures that could be viewed as a defense version of the Economic Security Promotion Act, such as the establishment of a fund to facilitate transfers of defense equipment and technology. We are considering whether to provide further information on these various measures in the future.

security" means "ensuring Japan's national interests, such as peace, security, and economic prosperity, by carrying out economic measures.[4] In addition, "Japan's national interests" that should be preserved and developed by Japan include not only "maintaining its sovereignty and independence, defending its territorial integrity, and securing the safety of the lives, person, and property of its nationals," but also "achieving the prosperity of Japan and its nationals through economic growth," "maintaining and strengthening an open and stable international economic order," and maintaining and protecting "universal values, such as freedom, democracy, respect for fundamental human rights, and the rule of law" and "international order based on international law" ("II. Japan's National Interests").

- The Security Strategy clarifies that Japan will take the following necessary economic measures to enhance Japan's self-reliance and secure the advantages and indispensability concerning its technology.

(i)	Steadily implementing and constantly reviewing the Economic Security Promotion Act,[5] and further reinforcing efforts in this regard;
(ii)	In regard to supply chain resilience, curbing excessive dependence on specific countries, carrying forward next-generation semiconductor development and manufacturing bases, and securing a stable supply of critical goods, including rare earth;
(iii)	Promoting capital reinforcement of private enterprises with critical goods and technologies, and strengthening the function of policy-based finance;
(iv)	Considering reviewing government procurement procedures, including those by local municipalities;
(v)	Considering expanding the scope of the prior screening system under the Economic Security Promotion Act;
(vi)	**Carrying out additional measures to ensure more appropriate management of sensitive data;**
(vii)	**Carrying out additional measures to ensure the safety and reliability of information and communication technology services;**
(viii)	**Examination on bolstering Japan's information security, including security clearance, by keeping in mind information security practices of leading countries and the needs of the industries;[6]**
(ix)	Considerations on further stepping up support and developing systems for information gathering, development, and fostering of advanced critical technologies for the purpose of fostering and preserving technology and other purposes;
(x)	Considerations on enhancing investment screening and export control;

4 The Act on the Promotion of Maintenance of Security Through Integrated Economic Measures (Act No. 43, 2022; the "**Economic Security Promotion Act**") does not define "economic security." However, in the course of deliberations on the bill, the former Minister of State for Economic Security Takayuki Kobayashi explained it as "ensuring the economic security of the state and its people" (House of Representatives Cabinet Committee Meeting No. 11, March 23, 2022, Answer by Minister of State Kobayashi, etc.). This has now been explicitly defined in the Security Strategy, which is a government document.

5 For more information on the Economic Security Promotion Act, please refer to our Newsletter (Contents of the Economic Security Promotion Act and its Impact on Foreign Companies and Designation of supported materials (specified critical materials) in relation to supply chain resilience)) and "50 Q&As on the Economic Security Promotion Act" by Yuki Sakurada in NBL magazine (NBL, No. 1226 (September 15, 2022) and No. 1227 (October 1, 2022)), etc.

6 In regard to (viii) considerations on bolstering Japan's information security, including security clearance, "Basic Policy on Economic and Fiscal Management and Reform 2022" (approved by the Cabinet Decision on June 7, 2022)" stated that "we will consider the necessary measures, including the development of a system for granting qualifications to those who handle critical information, based on the verification of specific cases in international joint research, etc."

(xi) Considerations on enhancing responses to forced technology transfers;
(xii) Considerations on further promoting research integrity;
(xiii) Considerations on implementing measures against talent drain; and
(xiv) Promoting effective efforts against economic coercion by foreign countries.

- In addition to the items related to the Economic Security Promotion Act enacted and promulgated in May 2022 or efforts related to supply chain resilience ((i), (ii), (iii), (v), and (ix)),[7] and "(x) investment screening and export control"[8] and "(xii) considerations in further promoting research integrity", which have been addressed by the Japanese government and are expected to be further addressed in the future, it is worth noting that measures related to data management and information and communication technology services, such as "(vi) measures to ensure more appropriate management of sensitive data"[9] and "(vii) measures to ensure the safety and reliability of information and communication technology services," which have not necessarily been mentioned as "economic security" issues in past government explanatory materials,[10] have been explicitly treated as "economic security" issues.
- In addition, it was also made clear that the Japanese government will consider taking measures to address the issue of forced technology transfers (referred to in (xi)), in relation to which serious concerns were expressed from the perspective of securing a level playing field in the G7 Trade Ministers'

---

7 In regard to "(ii) carrying out next-generation semiconductor development and manufacturing bases," we believe it is part of the government's efforts to develop advanced semiconductors, such as the Research and Development Business for Enhancing Post-5G Information and Telecommunication System Bases. In regard to "(v) considering expanding the scope of the prior screening system under the Economic Security Promotion Act," it is expected that the prior screening system for key infrastructure providers under the Economic Security Promotion Act will be enforced by February 2024, i.e., within one year and nine months from the date of promulgation thereof, and the details thereof will be prescribed through the formulation of government ordinances, etc. in the future. At the current stage, in which the prior screening system has not yet been enforced, the purpose of "considering expanding the scope" is unclear. It is worth noting, however, that this may suggest that, at least in the mid- to long-term, the scope of regulations may be expanded through a routine review of the prior screening system, even for infrastructure providers in areas other than the 14 infrastructure business areas (Article 50 of the Economic Security Promotion Act), such as electricity, gas, oil, waterworks, railroads, telecommunications, basic broadcasting, and financial services, which are currently listed in the Economic Security Promotion Act.

8 The U.S. National Security Strategy, released on October 12, 2022, also states that in regard to investment screening and export control, "we are countering intellectual property theft, forced technology transfer, and other attempts to degrade our technological advantages by enhancing investment screening, export controls, and counterintelligence resources" and "[w]e must ensure strategic competitors cannot exploit foundational American and allied technologies, know-how, or data to undermine American and allied security. We are therefore modernizing and strengthening our export control and investment screening mechanisms, and also pursuing targeted new approaches, such as screening of outbound investment, to prevent strategic competitors from exploiting investments and expertise in ways that threaten our national security," and these measures are viewed as being important from a security perspective.

9 "Overall Picture of the Economic Security Japan Seeks: Toward the Formulation of a New National Security Strategy," which is an opinion by the Economic Security Promotion Headquarters, Policy Research Council of the Liberal Democratic Party of Japan dated October 4, 2022, includes, as "development of a system for data management," development of a system for the use of cloud services based on the confidentiality of information (including the development of domestic cloud services), development of a system for the ownership of data, and flexible review of export and investment management targets (p. 5 of the same opinion).

10 For example, various measures set forth as "strengthening economic security" in the aforementioned "Basic Policy on Economic and Fiscal Management and Reform 2022" (approved by the Cabinet Decision on June 7, 2022)" (Chapter 3, 1(2)), etc.

Statement in September 2022,[11] and the issue of trade-related economic coercion (referred to in (xiv)), for which serious concerns were expressed in the same statement.[12]

- It should be noted that measures based on the Security Strategy are to be implemented from the perspective of strategy and sustainability, and in a timely and appropriate manner, under the control tower function of the National Security Council, and that within 10 years from now, necessary revisions are to be made when significant changes in the security environment and others are expected ("VIII. Duration, Evaluation, and Revision of the Strategy"); it is assumed that the implementation of measures above will be considered over the medium to long term, and are not necessarily intended to be implemented immediately.

2. Points to Note from a Cybersecurity Perspective

- In the "Basic Policy on Economic and Fiscal Management and Reform 2022" (approved by the Cabinet Decision on June 7, 2022), the section on "economic security" states, in regard to cybersecurity, that "in strengthening public-private partnerships and analytical capabilities to ensure cyber security in light of changes in international circumstances, the government will study necessary measures to be taken, including pursuing technological development and improving systems," thereby treating cybersecurity as an economic security issue. However, in the Security Strategy, as part of "Strengthening Efforts to Seamlessly Protect Japan in All Directions," cybersecurity, as with food security, energy security, and economic security, is categorized as a separate item independent of economic security issues. Moreover, the Security Strategy states that the Japanese government will improve the coordination between cybersecurity policies and other policies that contribute to the enhancement of cybersecurity, such as economic security and the enhancement of technical capabilities related to national security.
- Among these measures related to cybersecurity, it is worth noting that Japan has been recommended to introduce "active cyber defenses" in order to preemptively eliminate any possibility of serious cyberattacks that may result in security concerns on the part of the government and in relation to critical infrastructure, even if they do not amount to armed attacks, and to prevent the spread of damage in the

---

11 The statement stated that "[w]e will sustain and further step up our efforts working toward a level playing field through more effective use of existing tools, as well as developing appropriate new tools and stronger international rules and norms on nonmarket policies and practices. Our shared concerns include unfair practices, such as all forms of forced technology transfer, ..." The issue of forced technology transfers has been raised continuously since 2017, including by the United States in its investigation and actions under Section 301 of the Trade Act, requests for WTO consultations by the United States and the EU, and the Trilateral Meeting of Trade Ministers between the United States, Japan, and the European Union.

12 In the statement, it is stated that "[w]e are seriously concerned by the use of trade-related economic coercion, which undermines economic security, free and fair trade in the multilateral trading system, global security and stability and aggravates international tension. In order to fight attempts at economic coercion, reaffirming the G7 Leaders' commitment, we will enhance cooperation and explore coordinated approaches to address economic coercion . . . .." In December 2021, the EU published a proposal for regulations authorizing EU member states to take measures against economic coercion, and on December 7, 2022, established a WTO panel to address China's import restrictions on Lithuanian goods, among other issues. In addition, under the National Defense Authorization Act for Fiscal Year 2023, which was enacted in the U.S. on December 23, 2022, a cross-governmental task force on China's economic coercion was established, and it is assumed that the U.S. will counter this in cooperation with its allies, including Japan (Section 5514 of the same bill).

case of such attacks, as well as to establish systems for the implementation of such defenses.[13]

- The Security Strategy states that the government will consider how to implement necessary measures, including those detailed in (i) through (iii) below, in order to establish systems for the implementation of active cyber defenses:

(i) to advance efforts on information sharing to the Government in case of cyberattacks among the private sector including critical infrastructures, as well as coordinating and supporting the incident response activities for the private sector;

(ii) to take necessary actions to detect servers and others suspected of being abused by attackers through utilizing information on communications services provided by domestic telecommunications providers; and

(iii) For serious cyberattacks that pose security concerns against the Government, critical infrastructures, and others, to ensure that the Government will be given the necessary authorities that allow it to penetrate and neutralize attacker's servers and others in advance to the extent possible.

- The Security Strategy further states that, in order to implement and promote these measures, including active cyber defenses, the National center of Incident readiness and Strategy for Cybersecurity (NISC)[14] will be constructively restructured to establish a new organization which will comprehensively coordinate policies in the field of cybersecurity, in a centralized manner, and that the Japanese government will work

---

[13] The report dated November 22, 2022 (the "**Expert Council Report**") by the "Expert Council for Comprehensive Defense as National Power" (established by the Prime Minister's decision dated September 22, 2022) states that it is necessary to implement active cyber defenses in order to prevent cyberattacks, and it is not sufficient to deal with them after they have occurred. Specifically, it is stated that new systems should be established to enable the implementation of active cyber defenses by, for example, significantly strengthening the command post function that directs incident responses in a centralized manner in the field of cybersecurity for Japan as a whole (2(4)).

In addition, the LDP Opinion Dated April 26 describes "active cyber defenses" as "in general, not limited to passive countermeasures, but various activities, including information gathering intended to prevent attackers from achieving their objectives through active defensive measures such as counterattacks." The proposal also explains that in regard to the measures to be taken in the event of a cyberattack that does not lead to an armed attack, since especially in the cyber field the attacker has an overwhelming advantage, the LDP will promptly consider the implementation of "active cyber defenses" against attackers from the perspective of addressing the relationship between possible new cybersecurity legislation and existing laws, regulations, and the like, such as the Act on Prohibition of Unauthorized Computer Access, other institutional and technical viewpoints, and strengthening cooperation with the intelligence sector (Change in Fighting Methods (4)).

[14] Currently, the Order for Organization of the Cabinet Secretariat (Cabinet Order No. 219, 1957) stipulates that the NISC shall perform the following tasks (Article 4-2 of the Cabinet Order), and at least, the NISC does not seem to have been given the authority to comprehensively coordinate policies in the field of cybersecurity in a "centralized manner:"

(i) matters related to the monitoring and analysis of unauthorized activities against the information systems of the administrative branches of the Japanese government that are conducted through information and telecommunications networks or electromagnetic recording media;

(ii) matters related to investigations to determine the causes of serious events that have or may cause any hindrance to ensuring the cybersecurity in administrative branches (excluding matters under the charge of the Cabinet Intelligence and Research Office);

(iii) matters related to advice, provision of information, and other assistance necessary for ensuring cybersecurity of administrative branches;

(iv) matters related to audits necessary for ensuring cybersecurity of administrative branches; and

(v) in addition to those listed in (i) through (iv) above, matters related to ensuring cybersecurity in relation to the planning and drafting of the policies of administrative branches necessary to ensure uniformity in relevant policies and in relation to the general coordination of those policies (excluding matters under the charge of the National Security Secretariat, the Cabinet Public Relations Office, and the Cabinet Intelligence and Research Office).

on legislation and strengthen operations for the purpose of implementing these new measures in the field of cybersecurity.[15] However, it is unclear what form "active cyber defenses" will take in the future, and it is necessary to address concerns about infringement of citizens' rights, such as the secrecy of communications,[16] or to examine the relationship between possible new legislation and existing laws, regulations, and the like, such as the Act on Prohibition of Unauthorized Computer Access. Therefore, it is necessary to closely monitor the legislation and strengthening of operations regarding cybersecurity.

3. Future Outlook

As seen in 1. and 2. above, the Security Strategy includes various measures for economic and cybersecurity, which may have a broad impact on corporate activities. Since the Economic Security Promotion Act was enacted in Japan, the term "economic security" has become commonplace, and because Russia's invasion of Ukraine has resulted in delays and disruptions in the supply chain, 2022 could be viewed as the first year in which companies cannot help but recognize economic security as a matter which affects them directly. In 2023, the support system for ensuring the stable supply of critical materials under the Economic Security Promotion Act and the research and development support of critical technologies will be fully implemented, and the system for prior screening of key infrastructure is expected to be finalized. In the future, the companies involved will not only need to consider how to respond to these systems under the Economic Security Promotion Act, which will be in full operation, but also must continue to collect information on the matters for which laws and guidelines are expected to be established within the next 10 years, as set forth in the Security Strategy. Now that it has become clear that "globalization and interdependence alone cannot serve as a guarantee of peace and development across the globe," while recognizing that we are existing in "the most severe and complex post-war security environment" ("I. Purpose" and "IX. Conclusion"), it is necessary for companies to consider whether the responses to these measures set forth in the Security Strategy are necessary, and in some cases, discuss and confirm them with the competent authorities.

End

Public Relations Section, Nishimura & Asahi E-mail

15 Although the Basic Act on Cybersecurity (Act No. 104, 2014) is a cybersecurity-related law, it is unclear at this time whether the cybersecurity systems will be developed in the form of an amendment to this act or whether a new act is envisioned.

16 The Expert Council Report also states, "In studying the cybersecurity systems, it is necessary to make clear that the subject matter of such systems should be limited to matters involving security, and to eliminate concerns about infringement of the rights of citizens, such as the secrecy of communications" (2(4)).