Guidelines on Measures, etc. Under Act on Ensuring Appropriate Handling of Satellite Remote Sensing Data

December 29, 2017

National Space Policy Secretariat, Cabinet Office

Table of Contents

1. Introduction 2
2. Measures, etc. Relating to Use of SRS Instruments and SRS Data 3
   2.1. Measures, etc. relating to SRS Instruments 3
      2.1.1. Measures to Prevent Unauthorized Use of SRS Instruments 3
      2.1.2. Suspension of Function on Orbit Other Than Orbit For Which Application Was Made 6
      2.1.3. Measures necessary and appropriate to prevent receiving by a Receiving Station managed by a person whose certification was rescinded and being used as SRS Data 6
      2.1.4. Measures in Case of Fault, etc. 8
      2.1.5. Preparation and Management of Logs 8
      2.1.6. Termination Measure 11
   2.2. Measures, etc. relating to Handling of SRS Data 13
      2.2.1. Restriction on Method of Provision of SRS Data 13
      2.2.2. Order of Prohibition of Provision of SRS Data 19
      2.2.3. Safety Management Measures 20
      2.2.4. Preparation and Management of Logs 36
3. Review of Guidelines 38

[Explanatory Notes]

Unless otherwise provided, the terms used in these Guidelines have the meanings as defined in the Act and Enforcement Regulation. The abbreviations as used in these Guidelines have the following meanings:

- Act: Act on Ensuring Appropriate Handling of Satellite Remote Sensing Data (Act No. 77 of 2016)
- Enforcement Regulation: Regulation for Enforcement of the Act for Ensuring Appropriate Handling of Satellite Remote Sensing Data (Cabinet Office Order No. 41 of 2017)
- Enforcement Order: Order for Enforcement of the Act for Ensuring Appropriate Handling of Satellite Remote Sensing Data (Cabinet Order No. 282 of 2017)
- SRS Instruments: Satellite Remote Sensing Instruments
- SRS Data: Satellite Remote Sensing Data

1. Introduction

Matters necessary for the measures concerning the use of SRS Instruments and handling of SRS Data are provided in the Act and Enforcement Regulation. These Guidelines are intended to provide detailed explanations on such measures, etc.

2. Measures, etc. Relating to Use of SRS Instruments and SRS Data

2.1. Measures, etc. relating to SRS Instruments

2.1.1. Measures to Prevent Unauthorized Use of SRS Instruments

Article 8 of the Act (Measures to Prevent Unauthorized Use of Satellite Remote Sensing Instruments)

(1) For signals which are necessary to operate Satellite Remote Sensing Instruments and are provided for the use for information processing by computer, a Satellite Remote Sensing Instruments User must perform a conversion process through the use of computer and conversion codes (meaning codes used for a signal conversion process; hereinafter the same applies in this Article), so that it cannot be reconstructed without using conversion codes corresponding to the conversion codes used in the conversion process (referred to as "corresponding conversion code" in paragraph (5)), and take other necessary and appropriate measures specified by Cabinet Office Order to prevent the Use of Satellite Remote Sensing Instruments by a person other than the Satellite Remote Sensing Instruments User.

(2) For Electromagnetic Data of Detected Information transmitted from the Satellite Remote Sensing Instruments, a Satellite Remote Sensing Instruments User must perform a conversion process through the use of a computer and data conversion codes (meaning codes used for a conversion process of electronic or magnetic records; the same applies hereinafter), so that it cannot be reconstructed without using data conversion codes corresponding to the data conversion codes used in the conversion process (referred to as "corresponding data conversion code" in paragraphs (4) and (5)), or take other necessary and appropriate measures specified by Cabinet Office Order to prevent Electromagnetic Data of Detected Information sent from the Satellite Remote Sensing Instruments from being received by a Receiving Station other than the Receiving Station covered by license under Article 4, paragraph (1) and used as Satellite Remote Sensing Data.

(3) A Satellite Remote Sensing Instruments User must not provide a conversion code to any other person (if a person managing a Ground Radio Station for Command and Control is different from the Satellite Remote Sensing Instruments User, any person other than the person managing the Ground Radio Station for Command and Control).

(4) A Satellite Remote Sensing Instruments User must not provide a corresponding data conversion Code to any other person (if a person managing a Receiving Station is different from the Satellite Remote Sensing Instruments User, any person other than the person managing the Receiving Station).

(5) A Satellite Remote Sensing Instruments User must take measures for the prevention of divulgence, loss or damage of conversion codes, corresponding conversion codes, data conversion codes and corresponding data conversion codes (hereinafter referred to as "conversion codes, etc." in this paragraph), and any other necessary and appropriate measures specified by Cabinet Office Order for the safety management of the conversion codes, etc.

Article 10 of the Enforcement Regulation (Measures Specified by Cabinet Office Order as Referred to

in Article 8, paragraph (1) of the Act)

(1) The measures specified by Cabinet Office Order, as referred to in Article 8, paragraphs (1) and (2) of the Act, are any of the measures specified in the following items:

(i) making it impossible to reconstruct codes without the use of corresponding conversion codes or corresponding data conversion codes;

(ii) obtaining two or more frequencies and making communications depending on the use; and

(iii) taking a measure such that only a person authorized to use the Satellite Remote Sensing Instruments can operate the Operational Radio Station.

(2) The provisions of Article 7, paragraphs (1) and (2) apply mutatis mutandis to the measures specified by Cabinet Office Order as the measures necessary and appropriate for the safety management of conversion codes, etc. under Article 8, paragraph (5) of the Act.

■ Article 8, paragraph (1) of the Act

An SRS Instruments User is required to take measures specified in Cabinet Office Order so as to prevent any other person from using the SRS Instruments, for example, applying conversion process to signals necessary for operation of the SRS Instruments using conversion codes, and making it impossible to restore such signals without using the corresponding conversion codes.

The details of the measures are as provided in Article 10 of the Enforcement Regulation.

■ Article 8, paragraph (2) of the Act

An SRS Instruments User is required to take measures specified in Cabinet Office Order so as to prevent any Electromagnetic Data of Detected Information transmitted from such SRS Instruments from being received by any station other than the Receiving Station covered by the license of such SRS Instruments and used, for example, by applying a conversion process to such Electromagnetic Data of Detected Information using data conversion codes, and making it impossible to restore such Electromagnetic Data of Detected Information without using the corresponding data conversion codes.

The details of the measures are as provided in Article 10 of the Enforcement Regulation.

■ Article 8, paragraphs (3) to (5) of the Act

An SRS Instruments User may not provide conversion codes and corresponding data conversion codes to any other person.

In addition, an SRS Instruments User is required to take measures against divulgence, loss or damage of conversion codes, corresponding conversion codes, data conversion codes and corresponding data conversion codes. When taking such measures, the SRS

Instruments User is required to take the measures identical to the safety management measures for SRS Data pursuant to the provisions of Article 10, paragraph (2) of the Enforcement Regulation. For the details of such measures, please see the Guidelines 2.2.3, Safety Management Measures.2.2.3

2.1.2. Suspension of Function on Orbit Other Than Orbit For Which Application Was Made

> Article 9 of the Act (Suspension of Function Other than Orbit Pertaining to Application)
> If the Earth Orbiting Satellite installed with Satellite Remote Sensing Instruments that has been licensed under Article 4, paragraph (1) does not stay in the orbit licensed under that paragraph, a Satellite Remote Sensing Instruments User must immediately send a signal to the Satellite Remote Sensing Instruments from the Ground Radio Station for Command and Control to stop its function of detecting Ground Emitted Electromagnetic Waves, etc., and keep such function stopped until that Earth Orbiting Satellite is placed into the orbit licensed under that paragraph.

A Distinguishing Accuracy of Target of SRS Instruments varies to a significant degree with the orbit of an Earth Orbiting Satellite (in particular, altitude from earth's surface). If a user uses SRS Instruments on an orbit lower than that within the scope anticipated at the time of the application, the Distinguishing Accuracy of Target is improved, allowing the user to obtain data with higher accuracy than the data that was expected at the time of obtaining a license to use such SRS Instruments.
So, an SRS Instruments User must immediately send a signal to the SRS Instruments from the ground radio station for command and control when the Earth Orbiting Satellite installed with the SRS Instruments does not stay in the orbit pertaining to the license so as to stop its function of detecting Ground Emitted Electromagnetic Waves, etc., and must hold such function suspended until such Earth Orbiting Satellite is placed into the licensed orbit.

2.1.3. Measures necessary and appropriate to prevent receiving by a Receiving Station managed by a person whose certification was rescinded and being used as SRS Data

> Article 10 of the Act (Receiving Station Used for Receiving Electromagnetic Data of Detected Information)
> (1) When receiving Electromagnetic Data of Detected Information sent from the Satellite Remote

Sensing Instruments, a Satellite Remote Sensing Instruments User may not use any Receiving Stations other than those licensed under Article 4, paragraph (1) which is managed by the Satellite Remote Sensing Instruments User, Specified Data Handling Organization, or a person certified under Article 21, paragraph (1).

(2) When receiving Electromagnetic Data of Detected Information sent from the Satellite Remote Sensing Instruments, if a Satellite Remote Sensing Instruments User uses a Receiving Station which is managed by a person certified under in Article 21, paragraph (1), and if such certification is rescinded pursuant to the provisions of Article 25, paragraph (1) or Article 26, paragraph (1), the Prime Minister must promptly notify the Satellite Remote Sensing Instruments User to that effect.

(3) Upon receipt of the notice referred to in the preceding paragraph, the Satellite Remote Sensing Instruments User must take measures to ensure that Electromagnetic Data of Detected Information will not be sent to the Receiving Station from the Satellite Remote Sensing Instruments if receiving by the Receiving Station provided in that paragraph is possible and to ensure change the data conversion code, and take any other necessary and appropriate measures specified by Cabinet Office Order to prevent the Electromagnetic Data of Detected Information sent from Satellite Remote Sensing Instruments from being received by the Receiving Station and used as Satellite Remote Sensing Data.

Article 11 of the Enforcement Regulation (Measures Specified by Cabinet Office Order as Referred to in Article 10, paragraph (3) of the Act)

Article 11 (1) The measures specified by Cabinet Office Order, as referred to in Article 10, paragraph (3) of the Act, are any of the measures specified in the following items:

(i) to ensure that Electromagnetic Data of Detected Information is not transmitted to a Receiving Station provided in Article 10, paragraph (2) of the Act; and

(ii) to change data conversion codes.

When receiving Electromagnetic Data of Detected Information transmitted from SRS Instruments, the SRS Instruments User may not use any Receiving Station other than that managed by: (i) the SRS Instruments User, (ii) Specified Data Handlers, or (iii) person certified under Article 21, paragraph (1) of the Act.

In addition, if a Receiving Station managed by (iii) a person certified under Article 21, paragraph (1) of the Act is to be used, and if such person's certification is rescinded, a measure must be taken to make it impossible to receive Electromagnetic Data of Detected Information using the Receiving Station managed by such person.

The details of the measures are as provided in Article 11 of the Enforcement Regulation.

2.1.4. Measures in Case of Fault, etc.

Article 11 of the Act (Measures to be Taken in Case of Fault)

If a Satellite Remote Sensing Instruments User is unable to conduct the Use of Satellite Remote Sensing Instruments without taking any termination measures (meaning the Termination Measures provided in Article 15, paragraph (2); the same applies in Article 13, paragraph (6) and Article 14, paragraph (2)) due to the fault of the Satellite Remote Sensing Instruments or the Earth Orbiting Satellite installed with such Satellite Remote Sensing Instruments or any other reasons, and if there is no prospect of recovery, the Satellite Remote Sensing Instruments User must promptly make a notification to the Prime Minister to that effect pursuant to the provisions of Cabinet Office Order. In this case, the license under Article 4, paragraph (1) ceases to be effective.

Article 12 of the Enforcement Regulation (Notification in Case of Fault)

When a Satellite Remote Sensing Instruments User intends to make a notification under Article 11 of the Act, it must submit to the Prime Minister a written notification in Form 5.

When it becomes impossible to use SRS Instruments without taking a Termination Measure and it is unlikely that such system will recover (see the examples shown below), an SRS Instruments User must notify the Prime Minister of information such as the year, date, month of the occurrence of such fault, etc. (or, in the case where the year, date, month of the occurrence of a fault, etc. cannot be identified, the estimated year, date, month of the occurrence of such fault, etc.)
If it is possible to take a Termination Measure at the time of the occurrence of the fault, a user is required to do so in a certain manner.
The notification must be submitted using Form 5 of the Enforcement Regulation.

[Example of case where it is unlikely that the system will recover]

① A case where it is possible to judge that the function is unlikely to recover due to a fault, etc. of SRS Instruments from telemetry, etc.
② A case where there is no means for recovery, such as communication blackout.

2.1.5. Preparation and Management of Logs

Article 12 of the Act (Log)

(1) A Satellite Remote Sensing Instruments User must keep a log pursuant to the provisions of Cabinet Office Order (including electronic or magnetic records, if the electronic or magnetic records

have been prepared in lieu thereof; the same applies hereinafter), and specify matters specified by Cabinet Office Order concerning the status of the Use of Satellite Remote Sensing Instruments in the log.

(2) The log referred to in the preceding paragraph must be preserved pursuant to the provisions of Cabinet Office Order.

Article 13 of the Enforcement Regulation (Matters to be Stated in Logs)

(1) The matters specified by Cabinet Office Order, as referred to in Article 12, paragraph (1) of the Act, are as set forth in the following items:

(i) the date and time of sending signals for operation of a Satellite Remote Sensing Instruments, its contents and the place of the Ground Radio Station for Command and Control, etc. used for sending signals;

(ii) the date and time of recording the Electromagnetic Data of Detected Information, the scope of coverage, and letters, numbers, signs or any other codes for identification of these information (hereinafter referred to as "Identification Codes");

(iii) the date and time of ground transmission of Electromagnetic Data of Detected Information and the location of the Receiving Station used for receiving data;

(iv) status of processing or deleting the Electromagnetic Data of Detected Information; and

(v) If any Satellite Remote Sensing Data is to be provided to a third party, the Identification Code, category, date and time of provision of the Satellite Remote Sensing Data, the name of the recipient, and, the certificate number of the recipient if the recipient has obtained a certificate under Article 21, paragraph (4) of the Act.

(2) When a Satellite Remote Sensing Instruments User creates electronic or magnetic records for the logs under Article 12, paragraph (1) of the Act, it must do so by a method of recording the created electronic or magnetic records on a file stored in a computer used by it, or by a method of preparing the records using the means file which can securely record certain information by means of a magnetic disk, CD-ROM or any other means equivalent thereto (hereinafter referred to as "Magnetic Disks, etc.")

(3) A Satellite Remote Sensing Instruments User must record in the log the matters set forth in the items of paragraph (1) without delay, for each instance of transmission of signals for operation of Satellite Remote Sensing Instruments, recording of Electromagnetic Data of Detected Information, ground transmission of Electromagnetic Data of Detected Information, processing or deleting of Electromagnetic Data of Detected Information, or provision of Satellite Remote Sensing Data, for each Satellite Remote Sensing Instruments, and must keep the record for five years from the entry of the information.

An SRS Instruments User is required to keep a log to record the status of use of the SRS Instruments, and to preserve such log.
More concretely, in relation to the following matters, if there occurs any event which requires entry of information into the log, the user is required to make such entry without delay and to preserve the log for the designated period of time.

■Article 13, paragraph (1), items (i) to (iii) of the Enforcement Regulation
Use of SRS Instruments comprises: instruction for operation to the SRS Instruments (command transmission), recording by the SRS Instruments (imaging), and transmission of the records to the ground (downlink).
In order to verify that the Ground Radio Station for Command and Control used for the transmission and the Receiving Station used for receiving is appropriately used, it is necessary that these operations are accurately recorded.
To this end, a user is required to make an entry of information including the date and time of sending the signals for operation of SRS Instruments.

■Article 13, paragraph (1), item (iv) of the Enforcement Regulation
In order to make clear the status of Electromagnetic Data of Detected Information obtained through the use of SRS Instruments, it is necessary that its processing and deleting procedures are recorded in the log.
More concretely, a user is required to make entries into log the Identification Codes of the SRS Data to be processed and the details of such processing, in the case of processing; or the Identification Codes of the SRS Data to be deleted and the method and date and time of the deletion, in case of deletion.

■Article 13, paragraph (1), item (v) of the Enforcement Regulation
Provision of SRS Data to other parties must be made in accordance with the category of such data.
In order to verify that the SRS Data is provided in an appropriate manner, it is necessary that the category of data and the name of recipients, in addition to the Identification Codes of the SRS Data and date and time of its provision, are recorded in the log.

■Article 13, paragraph (2) of the Enforcement Regulation
Information on use of the SRS Instruments is generally prepared and managed on a computer. As such, preparation of such information by way of electronic or magnetic

records is acceptable.

■Article 13, paragraph (3) of the Enforcement Regulation

In order to verify that the SRS Instruments User is using the SRS Instruments in an appropriate manner, it is necessary that each the activities specified in the Enforcement Regulation is recorded in the log without delay.

Further, as the license for use of SRS Instruments is granted for the individual SRS Instruments, a user of two or more SRS Instruments is required to prepare a log for each of the SRS Instruments.

2.1.6. Termination Measure

(b) Termination Measure provided in Article 15 of the Act;

(1) A Satellite Remote Sensing Instruments User may terminate the Use of Satellite Remote Sensing Instruments at any time, in addition to the cases referred to in Article 13, paragraph (6), Article 14, paragraph (2), Article 16, paragraph (2) or Article 17, paragraph (2).

(2) When a Satellite Remote Sensing Instruments User terminates the Use of Satellite Remote Sensing Instruments, it must take any of the following measures (hereinafter referred to as "Termination Measures"), pursuant to the provisions of Cabinet Office Order, and make a notification to the Prime Minister of the contents of the measure taken without delay.

(i) measure to send a signal from the Ground Radio Station for Command and Control to the Satellite Remote Sensing Instruments to stop its function of detecting Ground Emitted Electromagnetic Waves, etc., or any other necessary measures specified by Cabinet Office Order to stop such function completely; or

(ii) measure to ensure that a signal is sent from the Ground Radio Station for Command and Control to the Satellite Remote Sensing Instruments to stop its function until a restart signal (meaning a signal necessary to recover the function of detecting Ground Emitted Electromagnetic Waves, etc. if the function has been suspended; the same applies hereinafter) is received and that a notification of information on the restart signal and the method of creation thereof is made to the Prime Minister, and any other necessary measures specified by Cabinet Office Order in order to ensure that the function cannot be restored unless the restart signal is received by Satellite Remote Sensing Instruments;

(3) When the Termination Measures are taken pursuant to the provisions of the preceding paragraph, the license under Article 4, paragraph (1) ceases to be effective.

(4) A person who has taken the Termination Measures set forth in item (ii) of paragraph (2) must not provide information on the restart signal under that item and the method of creating said signal to

any persons other than Specified User Organizations or a person who has been newly licensed under Article 4, paragraph (1) to conduct the Use of Satellite Remote Sensing Instruments pertaining to the Termination Measures.

Article 17 of the Enforcement Regulation (Measures to be Specified by Cabinet Office Order as Referred to in Article 15, paragraph (2), item (i) of the Act)

(1) The measures specified by Cabinet Office Order, as referred to in Article 15, paragraph (2), item (i) of the Act, are any of the measures specified in the following items:

(i) sending signals from a Ground Radio Station for Command and Control to the Satellite Remote Sensing Instruments subject to the measure to stop the function to detect Ground Emitted Electromagnetic Waves, etc.; or

(ii) sending signals from a Ground Radio Station for Command and Control to the Satellite Remote Sensing Instruments subject to the measure not to supply power.

(2) The measure specified by Cabinet Office Order, as referred to in Article 15, paragraph (2), item (ii) of the Act, is sending signals from a Ground Radio Station for Command and Control to the Satellite Remote Sensing Instruments subject to the measure to stop the function to detect the Ground Emitted Electromagnetic Waves, etc. until a restart signal is received, and the notification of information on the restart signal and the creation method thereof to the Prime Minister.

Use of SRS Instruments may be terminated any time, except for the cases referred to in Article 13, paragraph (6) of the Act (a case where a business transfer, merger or company split was implemented but an authorization of succession was not granted), Article 14, paragraph (2) of the Act (a case where a user is deceased but an authorization of succession was not granted), Article 16 of the Act (a case where a user was dissolved but an authorization of succession was not granted) or Article 17, paragraph (2) of the Act (a case where a license was rescinded).

Meanwhile, when terminating the use of SRS Instruments, unless the SRS Instruments' function to detect Ground Emitted Electromagnetic Waves, etc. is properly suspended, a person intending to use such SRS Instruments for an inappropriate purpose might operate the uncontrolled SRS Instruments without authorization and use such SRS Instruments in an inappropriate manner. Therefore, the Act requires that a measure be taken to appropriately stop SRS Instruments' function to detect Ground Emitted Electromagnetic Waves, etc. when terminating the use of the SRS Instruments. In such case, the details of measures must be reported to the Prime Minister without delay.

The details of the measures are as provided in Article 17 of the Enforcement Regulation.

2.2. Measures, etc. relating to Handling of SRS Data

2.2.1. Restriction on Method of Provision of SRS Data

Article 18 of the Act (Restriction on Provision of Satellite Remote Sensing Data)

(1) When providing the Satellite Remote Sensing Data to a person who obtained a certification under Article 21, paragraph (1) for the handling of Satellite Remote Sensing Data, a Satellite Remote Sensing Data Holder must do so after verifying that the recipient of such provision is a person who has obtained that certification, by requiring such recipient to present a certificate under paragraph (4) of that Article, clearly indicating the categories of the Satellite Remote Sensing Data specified by Cabinet Office Order as referred to in paragraph (1) of that Article, and provide the information using cryptography or any other method of transmission whereby it is not easy to restore the contents thereof or any other method specified by Cabinet Office Order as necessary and appropriate for prevention of acquisition and use of Satellite Remote Sensing Data by any person other than the recipient of the Satellite Remote Sensing Data, pursuant to the provisions of Cabinet Office Order.

(2) When providing the Satellite Remote Sensing Data to a Satellite Remote Sensing Instruments User (limited to those who have obtained a license under Article 4, paragraph (1) for the Use of Satellite Remote Sensing Instruments pertaining to the relevant Satellite Remote Sensing Data) or Specified Data Handling Organization, a Satellite Remote Sensing Data Holder must provide the data by clearly indicating to the recipient the categories of the Satellite Remote Sensing Data specified by Cabinet Office Order as referred to in Article 21, paragraph (1) and by the method specified by Cabinet Office Order referred to in the preceding paragraph, pursuant to the provisions of Cabinet Office Order.

(3) A Satellite Remote Sensing Data Holder may not provide the Satellite Remote Sensing Data except when such provision is made pursuant to the provisions of the preceding two paragraphs for the examination or research conducted by each House or by a committee of each House or research committee of the House of Councilors pursuant to the provisions of Article 104, paragraph (1) of the Diet Act (Act No. 79 of 1947) (including the as applied mutatis mutandis pursuant to Article 54-4, paragraph (1) of the same Act) or Article 1 of the Act on Witnesses' Oath, Testimony, etc. Before Both Houses of the Diet (Act No. 225 of 1947), litigation proceedings or any other court proceedings, an execution of judicial decisions, an investigation of criminal cases, or the audit by the Board of Audit, or in any other case equivalent thereto where such provision is necessary for the public interest as specified by a Cabinet Order, or such provision is carried out in an urgent situation when measures must be taken to rescue human life, for disaster relief or for other emergencies.

Article 20 of the Enforcement Regulation (Method of Provision of Satellite Remote Sensing Data)

(1) The method specified by Cabinet Office Order as the method necessary and appropriate for prevention of acquisition and use of Satellite Remote Sensing Data by any person other than the recipient of the Satellite Remote Sensing Data, as referred to in Article 18, paragraph (1) of the Act, is any of the measures specified in the following items:

(i) cryptography or any other method of transmission whereby it is not easy to restore the contents thereof; or

(ii) a method of encrypting Satellite Remote Sensing Data and recording it on Magnetic Disks, etc., and providing it by means of the Magnetic Disks, etc.

(2) When a Satellite Remote Sensing Data Holder provides Satellite Remote Sensing Data pursuant to the provisions of Article 18, paragraph (1) of the Act, it must require the recipient to present a certificate under Article 21, paragraph (4) of the Act in advance, and must clearly indicate the category of the Satellite Remote Sensing Data provided in Article 22.

(3) When a Satellite Remote Sensing Data Holder provides the Satellite Remote Sensing Data to a Satellite Remote Sensing Instruments User provided in Article 18, paragraph (2) of the Act pursuant to the provision of that paragraph, it must confirm the name of the Satellite Remote Sensing Instruments User and the name and type of the Satellite Remote Sensing Instruments in advance, and must clearly indicate the category of Satellite Remote Sensing Data provided in Article 22.

(4) The provisions of the preceding paragraph apply mutatis mutandis to the case of provision of Satellite Remote Sensing Data to a Specified Data Handling Organization pursuant to the provisions of Article 18, paragraph (2) of the Act. In this case, the phrase "the name of the Satellite Remote Sensing Instruments User and the name and type of the Satellite Remote Sensing Instruments" is deemed to be replaced with "the name of the Satellite Remote Sensing Instruments.

Article 21 of the Enforcement Regulation (Procedures in Case of Provision of Satellite Remote Sensing Data Due to Urgent Necessity)

(1) When a Satellite Remote Sensing Data Holder provided Satellite Remote Sensing Data due to urgent necessity for rescuing human lives, disaster relief or any other response to emergent situations (including the case of response through international cooperation) if a disaster (meaning a disaster provided in Article 2, item (i) of the Basic Act on Disaster Control Measures (Act No. 223 of 1958) occurred or is likely to occur, the Satellite Remote Sensing Data Holder must submit a document stating the following matters to the Prime Minister without delay.

(i) the details of the situation;

(ii) the background and process of provision of the Satellite Remote Sensing Data;

(iii) the category of the Satellite Remote Sensing Data;

(iv) the scope and period of the Satellite Remote Sensing Data; and

(v) the name of the recipient (including another recipients who received the data from the recipient).

(2) When submitting the document set forth in the preceding paragraph, a document clearly specifying the matters set forth in items (i) and (ii) of that paragraph and any other necessary documents must be attached.

Article 2 of the Act (Definitions)

In this Act, the meanings of the terms set forth in the following items are as provided respectively in those items:

(i) to (iv) (the rest is omitted.)

(v) "Specified User Organization" means a national governmental organization or local governmental organization prescribed by Cabinet Order as an entity capable of performing an appropriate Use of Satellite Remote Sensing Instruments.

(vi) (the rest is omitted.)

(vii) "Specified Data Handling Organization" means Specified User Organization and a national or local governmental organization in Japan or a governmental organization of a foreign country (meaning a country or region outside of Japan; the same applies hereinafter) prescribed by Cabinet Order as an entity capable of performing an appropriate handling of Satellite Remote Sensing Data.

(viii) (the rest is omitted.)

Article 1 of the Enforcement Order (National Governmental Organizations Specified by Cabinet Order as Referred to in Article 2, item (v) of the Act)

The national governmental organization to be specified by Cabinet Order, as referred to in Article 2, item (v) of the Act on Ensuring Appropriate Handling of Satellite Remote Sensing Data (hereinafter referred to as the "Act") is the Cabinet Secretariat.

Appended Table 1 of the Enforcement Order (Re: Article 2)

Cabinet Office

Fair Trade Commission

National Public Safety Commission

National Police Agency

Financial Services Agency

Ministry of Internal Affairs and Communications
Fire and Disaster Management Agency
Ministry of Justice
Public Prosecutors Office
Public Security Examination Commission
Public Security Intelligence Agency
Ministry of Foreign Affairs
Ministry of Finance
National Tax Agency
Ministry of Education, Culture, Sports, Science and Technology
Sports Agency
Agency for Cultural Affairs
Ministry of Health, Labour and Welfare
Ministry of Agriculture, Forestry and Fisheries
Forestry Agency
Fisheries Agency
Ministry of Economy, Trade and Industry
Agency for Natural Resources and Energy
Small and Medium Enterprise Agency
Ministry of Land, Infrastructure, Transport and Tourism
Meteorological Agency
Japan Coast Guard
Ministry of the Environment
Nuclear Regulation Authority
Ministry of Defense
Acquisition, Technology and Logistics Agency
Board of Audit of Japan

■ Article 18, paragraph (1) of the Act

For handling SRS Data, appropriate management according to data categories is necessary. In addition, if the data is not provided in an appropriate manner, Ensuring of the Peace of the International Community, etc. may be harmed as a result of divulgence, etc. of SRS Data.

Therefore, for the provision of SRS Data, it is necessary to prevent divulgence to third parties by checking a certificate possessed by the recipient, clearly specifying the data of appropriate categories, and providing such data in an appropriate manner.

As SRS Data is electronic or magnetic records, provision by way of telecommunication or portable storage media is anticipated. In such case, there is a risk of divulgence to third parties if appropriate measures are not taken. Therefore, for providing SRS Data, prevention of divulgence to third parties is required by taking measures such as encryption.
The method of providing SRS Data as referred to above is set forth in Article 20, paragraph (1) of the Enforcement Regulation.

■ Article 8, paragraph (2) of the Act
For providing SRS Data to an SRS Instruments User (limited to an SRS Instruments User pertaining to such SRS Data), it is necessary to verify that the recipient is the user of such system by confirming the name of such SRS Instruments User or the name and category of such SRS Instruments.
For providing SRS Data to a Specified Data Handler, it is necessary to verify that the recipient is a Specified Data Handler by confirming the name of such Specified Data Handler.
In Article 2, paragraph (1) of the Enforcement Order, national or local public organizations listed in item (i) and (ii) of the paragraph shall take appropriate measures equivalent to that Satellite Remote Sensing Data Holder shall take the safety management measures as specified by the Enforcement Regulation, according to Article 20 of the Act.
Then Satellite Remote Sensing Data Holder is necessary to confirm regulations of the national or local public organization if the organization has measures equivalent to the safety management measures before providing SRS Data to the organization, by inquiring with Cabinet Office about the organization if necessary.

The method of providing SRS Data as referred to above is as set forth in Article 20, paragraphs (3) and (4) of the Enforcement Regulation.

■ Article 18, paragraph (3) of the Act
For the examination or research conducted by each House, court proceedings, execution of judicial decisions, investigation of criminal cases or any other case being equivalent thereto where such provision is necessary for the public interest as specified by a Cabinet Order, or for the response to an urgent situation where measures must be taken to rescue human life, disaster relief or for other emergencies, restriction on provision of SRS Data may be detrimental to the execution of duties. In these cases, provision of

SRS Data is permitted under Article 18, paragraph (3) of the Act.
In the case of the urgent necessity for responding to the rescue of human life, disaster relief or any other emergencies, SRS Data may be provided without taking measures such as confirmation of a certificate of the recipient or using a communication method incapable of recovering secret codes or any other details thereof, which are usually required when providing SRS Data, as such measures would cause difficulties for swift response to disaster, etc.
In this connection, under the Enforcement Regulation, a SRS Data Holder who provided SRS Data due to "urgent necessity for rescuing human lives, disaster relief or any other response to emergent situations (including the case of response through international cooperation)" in the case where "a disaster (meaning a disaster provided in Article 2, item (i) of the Basic Act on Disaster Control Measures (Act No. 223 of 1958) occurred or is likely to occur," is required to submit information summarizing the details of such data to the Prime Minister.
Therefore, whether the provision of SRS Data falls under the aforementioned cases is determined based on whether an "urgent necessity for rescuing human lives, disaster relief or any other response to emergent situations" exists in the case where "wind storms, tornados, torrential rains, heavy snows, floods, landslides, debris flows, storm surges, earthquakes, tsunamis, volcanic eruptions and any other abnormal natural phenomena, large-scale fire or explosion, or any other damage caused by events specified by a Cabinet Order as events with the equivalent degree of damage (e.g. emission of large amount of radioactive substance, sinking of a vessel causing distress to a large number of people, or any other large-scale accidents)" as provided in Article 1, item (i) of the Basic Act on Disaster Control Measures occurred or is likely to occur.
Such determination is made considering the individual and specific circumstances of the case. For example, the following cases would be considered to satisfy the conditions.

- a case of providing SRS Data to respond to a disaster, in the case where a forecast or warning of such disaster has been made (including the case of using SRS Data for discussion of such forecast or warning).
- a case where a disaster response headquarters relating to such disaster is established, and where SRS Data is provided for the purpose of responding to such disaster.
- a case where SRS Data is provided for the purpose of responding to a disaster within the international framework among space organizations and disaster prevention organizations relating to a disaster (e.g. the Sentinel Asia, the International Charter "Space and Major Disasters")

2.2.2. Order of Prohibition of Provision of SRS Data

Article 19 of the Act (Order Prohibiting Provision of Satellite Remote Sensing Data)

(1) If the Prime Minister believes on the sufficient ground that the use of Satellite Remote Sensing Data is likely to cause adverse effect on Ensuring of Peace of the International Community, etc., the Prime Minister may issue an order to a Satellite Remote Sensing Data Holder (excluding a natural person who has neither domicile nor residence in Japan or a corporation or any other organization which does not have a principal office in Japan that handles Satellite Remote Sensing Data in a foreign country (hereinafter referred to as a "Foreign Handler")) to prohibit provision of the Satellite Remote Sensing Data designating the scope and time period.

(2) The prohibition order under the preceding paragraph must be limited to the minimum extent required for the Ensuring of Peace of the International Community, etc.

(3) The provisions of the preceding two paragraphs apply mutatis mutandis to a Satellite Remote Sensing Data Holder (limited to a Foreign Handler). In this case, the term "to prohibit provision" in paragraph (1) is deemed to be replaced with "not to provide", and the term "issue an order to" in the preceding paragraph is deemed to be replaced with "request."

Article 3 of the Enforcement Regulation (Standards Specified by Cabinet Office Order as Referred to in Article 2, item (vi) of the Act)

(Standards to be Specified by Cabinet Office Order as Referred to in Article 2, item (vi) of the Act)

Categories	Standards
(i) Raw data	(a) for data recorded by an optical sensor, data with Distinguishing Accuracy of Target not exceeding 2 meters, which is within five years after the recording. (b) for data recorded by a SAR sensor, data with Distinguishing Accuracy of Target not exceeding 3 meters, which is within five years after the recording. (c) for data recorded by a hyperspectral sensor, data with Distinguishing Accuracy of Target not exceeding 10 meters and detectable wavelength bands exceeding 49, which is within five years after the recording. (d) for data recorded by a thermal infrared sensor, data with Distinguishing Accuracy of Target not exceeding 5 meters, which is within five years after the recording.

(ii) Standard data	(a) for data recorded by an optical sensor, data with Distinguishing Accuracy of Target less than 25 centimeters. (b) for data recorded by a SAR sensor, data with Distinguishing Accuracy of Target less than 24 centimeters. (c) for data recorded by a hyperspectral sensor, data with Distinguishing Accuracy of Target not exceeding 5 meters and detectable wavelength bands exceeding 49. (d) for data recorded by a thermal infrared sensor, data with Distinguishing Accuracy of Target not exceeding 5 meters.

(2) Notwithstanding the provisions of the preceding paragraph, the standards specified by Cabinet Office Order, as referred to in Article 2, item (vi) of the Act pertaining to Satellite Remote Sensing Data subject to an order prohibiting provision pursuant to the provisions of Article 19, paragraph (1) of the Act, are to be specified by the Prime Minister by a public notice.

Prohibition of provision of SRS Data under Article 19, paragraph (1) of the Act is ordered in case where there is a sufficient reason to believe that such provision is likely to cause harm to Ensuring of the Peace of the International Community, etc.
As the standards for the SRS Data subject to the prohibition are determined depending on the circumstances of individual and specific cases, it is difficult to set specific standards in advance.
Therefore, such standards are to be determined by the Prime Minister in a public notice depending on the circumstances of individual and specific cases.

2.2.3. Safety Management Measures

Article 6 of the Act (Requirements for License)

The Prime Minister may not grant the license under Article 4, paragraph (1), unless the Prime Minister finds that the application for the license under that paragraph meets all of the following requirements:

(ii) measures for prevention of divulgence, loss or damage of Satellite Remote Sensing Data and any other necessary and appropriate measures to be specified by Cabinet Office Order for the safety management of the Satellite Remote Sensing Data have been taken;

Article 20 of the Act (Safety Management Measures for Satellite Remote Sensing Data)

A Satellite Remote Sensing Data Holder must take measures for prevention of divulgence, loss or

damage of Satellite Remote Sensing Data and any other necessary and appropriate measures specified by Cabinet Office Order for the safety management of the relevant Satellite Remote Sensing Data.

Article 7 of the Enforcement Regulation (Measures Specified by Cabinet Office Order as Referred to in Article 6, item (ii) of the Act)

(1) The measures specified by Cabinet Office Order, as referred to in Article 6, item (ii) and Article 20 of the Act, are as specified in the lower column of the following table, in accordance with the categories of Satellite Remote Sensing Data respectively specified in the upper column of the table.

Categories of Satellite Remote Sensing Data	Measures
(i) Raw data	(a) Organizational safety management measures (i) that a basic policy for safety management of the Satellite Remote Sensing Data is established. (ii) that the responsibilities and authorities as well as businesses of person in charge of handling Satellite Remote Sensing Data are made clear. (iii) that an organization for handling business in case of divulgence, loss or damage of Satellite Remote Sensing Data is established. (iv) that regulations on safety management measures have been established and implemented, and operation of such regulations is being assessed and improved. (b) Human safety management measures (i) that confirmation is made that the person in charge of handling Satellite Remote Sensing Data does not fall under any of Article 5, items (i) to (iv) and Article 21, paragraph (3), item (i)(a) to (d) of the Act; (ii) that a person in charge of handling Satellite Remote Sensing Data has taken has taken measures to ensure that information on Satellite Remote Sensing Data handled by such person in the course of business and any other special confidential information (meaning unpublished information which such person may learn in the course of business) will not be used for any purpose other than for the ensuring of appropriate operation of such business or any other purpose found to be necessary. (iii) that necessary education and training are provided to a person

	in charge of handling Satellite Remote Sensing Data. (c) Physical safety management measure (i) that facilities for handling Satellite Remote Sensing Data are clearly distinguished. (ii) that measures have been taken to restrict entry into and bringing any device into facilities for handling Satellite Remote Sensing Data. (iii) that for a computer and portable memory device (meaning a portable media or device capable of being inserted into or connected to a computer or its peripheral equipment to store information; hereinafter the same applies in this paragraph), in order to prevent theft, loss or any other accident, fixing the edge of a computer with a wire or any other necessary physical measures have been taken. (d) Technical safety management measures (i) that appropriate measures have been taken for facilities for handling Satellite Remote Sensing Data so as to prevent unauthorized access (meaning unauthorized access as provided in Article 2, paragraph (4) of the Act on Prohibition of Unauthorized Computer Access (Act No. 128 of 1999). (ii) that measures have been taken to restrict a portable memory device from being connected with a computer or its peripheral equipment. (iii) that operations of computers and terminals relating to the handling of Satellite Remote Sensing Data have been recorded. (iv) that for transfer or telecommunication transmission of Satellite Remote Sensing Data, encryption or any other necessary measures for the appropriate protection of Satellite Remote Sensing Data have been taken. (v) that for processing of Satellite Remote Sensing Data, necessary measures have been taken to ensure that such processing is implemented in an appropriate manner.
(ii) Standard data	(a) Organizational safety management measures Same as (a) for the paragraph of raw data. (b) Human safety management measures Same as (a) for the paragraph of raw data.

	(c) Physical safety management measure Same as (a) for the paragraph of raw data.

(2) If a Satellite Remote Sensing Instruments User and Satellite Remote Sensing Data Holder manages the business of handling of Satellite Remote Sensing Data, in whole or part, by the use of external storage service through telecommunication lines, it must expressly provide for the following matters in a contract with the business providing the service (hereinafter referred to as a "service provider" in this paragraph) relating to the use of the service.

(i) that the measures equivalent to those provided in the preceding paragraph are to be taken; and

(ii) that Satellite Remote Sensing Data is not to be stored on a computer located in any of the following countries or regions:

(a) the regions specified in Appended Table 3-2 or 4 of the Export Order; or

(b) the countries or regions determined by a resolution of the United Nations General Assembly or Security Council as being responsible for the occurrence of situations threatening the peace and security of the international community;

(iii) that, upon the cancellation or expiration of the contract, deletion or return of Satellite Remote Sensing Data or any other necessary measures are to be taken; and

(iv) that, if the service provider entrusts all or part of its business to a third party, a contract for the business entrustment provides for a condition that the entrusted party must comply with the matters specified in the preceding three items and that the entrusted party must take any other measures to perform the business in an appropriate and accurate manner.

(3) The measures provided in the preceding two paragraphs do not apply to Satellite Remote Sensing Data to be provided for necessary purposes in view of public interest or for the urgent necessity for rescuing human lives, disaster relief or any other emergencies, as provided in Article 18, paragraph (3) of the Act.

■Article 7, paragraph (1) of the Enforcement Regulation

SRS Instruments Users and SRS Data Holders must take necessary and appropriate measures to prevent divulgence, loss or damage of SRS Data it handles and to otherwise manage the safety of SRS Data.

More specifically, it is necessary to implement, in an appropriate manner, "organizational safety management measures" including establishment of organizational structure, "human safety management measures" including supervision and education of persons engaged in handling of SRS Data, "physical safety management measures" including management of sections for handling SRS Data and prevention of theft of computers and electronic media, and "technical safety

management measures" including prevention of unauthorized access from outside and access control.
The following examples of concrete methodologies for the safety management measures are not intended to be limited to only the following.

2.2.3.1. Organizational safety management measures

Organizational safety management measures mean the following safety management measures at the organizational level.

① Establishment of a basic policy for safety management of SRS Data.
② Clearly specifying the authorities and responsibilities as well as the duties of a person in charge of handling SRS Data.
③ Establishment of an organization for business handling in case of divulgence, destruction or damage of SRS Data.
④ Establishment and operation of regulations on safety management measures for SRS Data, as well as assessment and improvement of the operation thereof.

[Applicable persons]

- SRS Instruments User
- SRS Data Holder (Raw Data/Standard Data)

(i) that a basic policy for safety management of the Satellite Remote Sensing Data is established.

In order to commit to safety management of SRS Data at the organizational level, it is important to provide for a basic policy so as to ensure that persons in charge of handling SRS Data understand such policy.
For this purpose, when drafting a basic policy, SRS Instruments Users and SRS Data Holders are required to make clear the business of handling SRS Data and its position within the organization, present a basic approach for safety management of SRS Data, and ensure compliance with laws, regulations, rules, etc. on SRS Data.

[Examples of methods]

For example, the following items can be provided in the basic policy:

① Compliance with applicable laws, regulations and rules
② Item relating to safety management measures

(ii) that the responsibilities and authorities as well as businesses of person in charge of handling Satellite Remote Sensing Data are made clear.

Safety management of SRS Data is achieved by making clear the scope of persons in charge of handling SRS Data, and by such persons understanding and fulfilling their respective authorities and responsibilities. In particular, it is important that persona who are determined to be responsible for the safety management of SRS Data understand the importance of the safety management of SRS Data.
To this end, it is necessary to make clear the scope of persons engaged in the handling of SRS Data and their respective authorities and responsibilities by way of a list, etc., and to establish organizations and structures as may be necessary.
"Persons in charge of handling SRS Data" mean officers of SRS Instruments Users and SRS Data Holders engaged in the business of handling of SRS Data (directors, executive officers, auditors, etc.) or their employees having authorities and responsibilities relating to such business, and persons engaged in the business of handling SRS Data under direct or indirect supervision of these persons (e.g. employees of such entity (full-time employees, contract workers, non-regular workers, part-time workers, etc.), and employees of other entities doing business pursuant to an entrustment contract).

[Examples of methods]

① Appointing a person responsible for the business of handling SRS Data and clearly specifying such person's responsibilities.
② Clearly specifying a person in charge of handling SRS Data and such person's roles.
③ Clearly specifying the scope of SRS Data to be handled by the person in charge of handling SRS Data.
④ Clearly specifying allocation of roles and responsibilities of each section, in the case where SRS Data is handled by two or more sections.

(iii) that an organization for handling business in case of divulgence, loss or damage of Satellite Remote Sensing Data is established.

In the case where the occurrence of divulgence, destruction or damage of SRS Data or indication thereof is discovered, the situation must be immediately identified at the

organizational level, and measures including prevention of collateral damage or recurrence of similar incidents must be taken.
For such purpose, SRS Instruments Users and SRS Data Holders are required to establish internal structures necessary for ensuring that such measures are implemented in an appropriate and swift manner.

[Examples of methods]

① Establishment of a reporting structure from a person handling SRS Data to a supervisor, in the case where a fact of violation of applicable laws and regulations or the indication thereof is discovered.
② Investigation into factual relationships and identification of cause.
③ Clearly specifying the person in charge of response to accidents and the supervisor.
④ Creation of a single point of contact for reporting in the case of occurrence of incidents including divulgence.
⑤ Discussion and determination of measures to prevent recurrence.
⑥ Report on factual situations and measures to prevent recurrence, etc.

(iv) that regulations on safety management measures have been established and implemented, and operation of such regulations is being assessed and improved.

For safety management of SRS Data, it is important to ensure the efficacy thereof.
For such purpose, SRS Instruments Users and SRS Data Holders are required to provide for regulations setting forth the details of the following "human safety management measures," "physical safety management measures" and "technical safety management measures" in addition to these "organizational safety management measures," ensure that persons engaged in handling of SRS Data understand these, and identify and analyze the status of implementation of such regulations and take improvement measures as may be necessary.

[Examples of methods]
For example, the following items can be provided in the regulations:

① Organizational safety management measures
   a) Establishment of a basic policy for safety management of SRS Data
   b) Establishment of organizational structure
   c) Operation in accordance with Handling Regulations, etc.

d) Establishment of structure to respond to divulgence incident, etc.
e) Review of safety management measures

② Human safety management measures
a) Supervision of persons in charge of handling SRS Data
b) Education of persons in charge of handling SRS Data

③ Physical safety management measure
a) Management of facilities for handling SRS Data
b) Restriction of access to facilities for handling SRS Data
c) Prevention of theft of computers, electronic devices, etc.

④ Technical safety management measures
a) Prevention of unauthorized access from outside
b) Control of access, and identification and authorization of persons with access
c) Recording of operations
d) Prevention of divulgence of information
e) Management of appropriate processing of SRS Data

<Attachments>

① Organization chart
② List of persons in charge of handling SRS Data

2.2.3.2. Human safety management measures

Human safety management measures mean the following safety management measures at human level.

① Confirmation that persons in charge of handling SRS Data do not fall under any disqualifying conditions.
② Prohibition of use of confidential information relating to SRS Data other than for the prescribed purpose by any person handling SRS Data.
③ Circulation of internal regulations and implementation of education and training for persons in charge of handling SRS Data.

[Applicable persons]
SRS Data User, SRS Data Holder (Raw Data/Standard Data)

(i) that confirmation is made that the person in charge of handling Satellite Remote Sensing Data does not fall under any of Article 5, items (i) to (iv) and Article 21, paragraph (3), item (i)(a) to (d) of the Act

For SRS Instruments Users and SRS Data Holders, and officers and employees having authorities and responsibilities relating to the business of handling SRS Data, a confirmation is to be made as to whether these persons fall under any disqualifying conditions in the process of examination for license and certification; however, persons other than the above who handle SRS Data are not examined.
Therefore, SRS Instruments Users and SRS Data Holders are required to confirm within their organizations that persons engaged in handling of SRS Data do not fall under any disqualifying conditions.

[Examples of methods]
Employer, etc. is to confirm that persons engaged in the handling of SRS Data within the organization do not fall under any disqualifying conditions by way of a commitment letter or confirmation letter.

(ii) that a person in charge of handling Satellite Remote Sensing Data has taken has taken measures to ensure that information on Satellite Remote Sensing Data handled by such person in the course of business and any other special confidential information (meaning unpublished information which such person may learn in the course of business) will not be used for any purpose other than for the ensuring of appropriate operation of such business or any other purpose found to be necessary.

SRS Data involves the risk of harming the Ensuring of the Peace of the International Community, etc. and therefore requires appropriate safety management. As such, SRS Instruments Users and SRS Data Holders need to take measures to ensure that confidential information pertaining to the SRS Data they handle in the course of business will not be used for any other purpose.

[Examples of methods]

① Conclusion of non-disclosure contract upon recruiting employees or execution of service contract
Preferably, a non-disclosure provision under an employment contract or service contract should remain effective for a certain period even after the termination of the contract.

② Establishment of regulations on the measures in case of violation of a non-disclosure contract

(iii) that necessary education and training are provided to a person in charge of handling Satellite Remote Sensing Data.

Even if regulations on safety management of SRS Data are established in an appropriate manner, it is impossible to achieve appropriate management if the contents of such regulations are not understood and complied with by persons engaged in the handling of SRS Data.
Therefore, SRS Instruments Users and SRS Data Holders are required to provide education and training for persons engaged in handling of SRS Data to gain deeper understanding as to the appropriate handling of SRS Data.

[Examples of methods]

① Regular training on points in attention relating to applicable laws and regulations, rules, etc.
② Implementation of necessary and appropriate education and training for persons in charge of handling SRS Data.

2.2.3.3. Physical safety management measures

Physical safety management measures mean the following safety management measures at physical level.

① Clearly designating facilities for handling SRS Data.
② Control of entry into and exit from facilities and bringing of equipment into facilities
③ Prevention of theft, etc. by physical protection of equipment and device

[Applicable persons]

SRS Data User, SRS Data Holder (Raw Data)

(i) that facilities for handling Satellite Remote Sensing Data are clearly distinguished.

If SRS Data is obtained by any person intending to use it for an inappropriate purpose, due to leaking and other reasons, Ensuring of the Peace of the International Community, etc. may be harmed.

Therefore, SRS Instruments Users and SRS Data Holders are required to control entry into and exit from facilities, restriction of bringing equipment into or taking it out from facilities, and, in order to ensure that these measures are implemented in an appropriate manner, clearly designate facilities for handling of SRS Data.

[Examples of methods]

① Establishment of wall, door with lock, partition, etc.
② Clearly designating facilities for handling of SRS Data in regulations, etc.
③ Determine the scope of facilities taking into account the actual status of operation, and only the scope which is capable of being managed in an appropriate manner should be designated.
④ In the case of handling SRS Data at a portable facility (e.g. vehicle mounted earth station), specify information enabling clear identification of the equipment, such as the name of such equipment

(ii) that measures have been taken to restrict entry into and bringing any device into facilities for handling Satellite Remote Sensing Data.

If facilities for handling SRS Data and server system for storing such data and terminals are located in the environment enabling contact by unspecified, multiple persons, there is a risk of impersonation by a person with improper intent or physical destruction of the system, as well as divulgence of information by unauthorized transfer of data from server rooms and terminals.
Therefore, SRS Instruments Users and SRS Data Holders are required to take measures for control of entry into and exit from facilities handling SRS Data and bringing device into such facilities, so as to secure safety of SRS Data they handle.
The term "device" means a portable information communication/storage device, and any other devices with function of storing electronic or magnetic records.

[Examples of methods]

① Creation of control system by such means as IC cards and number keys
② Record of entry/exit in case of control by means of lock (creation of entry/exit management list)
③ Installing locker, etc. for storing devices outside the facilities for handling data, and restricting bringing devices into the facilities.

(iii)that for a computer and portable memory device (meaning a portable media or device capable of being inserted into or connected to a computer or its peripheral equipment to store information; hereinafter the same applies in this paragraph), in order to prevent theft, loss or any other accident, fixing the edge of a computer with a wire or any other necessary physical measures have been taken.

Even if entry into and exit from facilities is controlled or bringing of equipment into facilities is restricted, it is meaningless if a computer handling SRS Data or portable memory device storing SRS Data located in such facilities is physically taken out from facilities.
Therefore, SRS Instruments Users and SRS Data Holders are required to take physical measures to prevent such computers and portable memory device from being taken out from facilities.

[Examples of methods]

① Keeping portable memory device storing SRS Data in a lockable cabinet, library, etc., and manage preparation and quantities thereof.
② In the case where the information system for handling of SRS Data is operated only with equipment, fixing such equipment by anti-theft wire lock.
③ Prohibiting leaving on desks, etc. media storing SRS Data and portable computers
④ Ensure that workers activate passwords and screen savers when leaving their desks

2.2.3.4. Technical safety management measures

Technical safety management measures mean the following technical management measures at the technical level.

① Appropriate measures for prevention of unauthorized access
② Measures relating to restriction of connection of portable memory devices to computers, etc. for handling SRS Data
③ Recording of operations of computers and terminal devices
④ Encryption of SRS Data at the time of transfer and transmission and any other necessary protective measures
⑤ Management of appropriate processing of SRS Data

[Applicable persons]
SRS Data User, SRS Data Holder (Raw Data/Standard Data)

(i) that appropriate measures have been taken for facilities for handling Satellite Remote Sensing Data so as to prevent unauthorized access (meaning unauthorized access as provided in Article 2, paragraph (4) of the Act on Prohibition of Unauthorized Computer Access (Act No. 128 of 1999).

Possibility of divulgence, etc. of SRS Data increases if any persons other than those handling SRS Data have access to SRS Data or if there is deficiency in the security measures of the information system.
Therefore, SRS Instruments Users and SRS Data Holders are required to restrict access to computers for handling SRS Data, and to appropriately manage information which identifies persons engaged in handling of SRS Data. In addition, measures must be also taken against possible attacks concerning vulnerabilities of computer security.

[Examples of methods]

① Limiting the persons with authority to give access to SRS Data and the authority to be granted to such persons
② Verifying the effectiveness of the access control function introduced into the information system for handling SRS Data (for example, checking vulnerabilities of OS and web applications)
③ Identification by a user ID, password, one-time password, IC card, etc. (note that user ID, etc. is to be provided so as to identify individual persons handling data).
    * In order to prevent unauthorized access, when creating passwords, take measures such as prohibiting passwords identical with user IDs, setting the effective period of passwords, restricting reuse of the identical or similar passwords, setting a minimum number of characters of passwords, and suspending IDs in the case of fault in log-in attempts exceeding more than a certain number.
④ Setting firewalls, etc. at the connecting point of the information system and outside network.
⑤ Installing anti-virus software and verifying of effectiveness and stability of such software (e.g. confirming updating of pattern files and hotfix)
⑥ Applying hotfix for security measures (namely, security patch) to operating

systems (OS), middleware (e.g. DBMS), applications, etc. to computers and servers.

⑦ Preventing installation of software not authorized by the organization.

(ii) that measures have been taken to restrict a portable memory device from being connected with a computer or its peripheral equipment.

For measures to prevent SRS Data from being taken out from facilities without authorization, it is important to restrict access to computers for handling SRS Data; however, unauthorized acquisition of data is also possible by way of connecting with external storage devices such as external hardware, CD-Rs and USB flash drives.
Therefore, SRS Instruments Users and SRS Data Holders are required to take measures to restrict connection of portable memory devices to computers for handling SRS Data and their peripheral equipment.

[Examples of methods]

① Restriction and management of connection of external memory devices, such as CD-Rs and USB flash drives.

② Restriction and management of connection of equipment with a storage function, such as smartphones and PCs.

(iii)that operations of computers and terminals relating to the handling of Satellite Remote Sensing Data have been recorded.

Recording of operation means recording of the history of operation and user access of the system and any other necessary information.
Such recording is serve as important information for detecting security incidents such as unauthorized access and unauthorized operation by a third party with malicious intent (including the indication thereof). Grasping such information is important as such information is useful for identification of the cause when any incidents such as information divulgence occur.
Therefore, SRS Instruments Users and SRS Data Holders are required to keep records of operations of information systems in an appropriate manner, and ensure that such records are stored in the environment enabling appropriate preservation without the risk of being tampered with.

[Examples of methods]

① Preservation of status of use of the information system for handling SRS Data (e.g. log-in history, access logs) and regular-basis monitoring
② Monitoring of access to SRS Data (including the details of operations)
③ Measures to prevent alteration and unauthorized deletion of collected logs
④ Monitoring access to the information system for handling SRS Data from outside by the use of an intrusion detection system, intrusion protection system, etc.

(iv) that for transfer or telecommunication transmission of Satellite Remote Sensing Data, encryption or any other necessary measures for the appropriate protection of Satellite Remote Sensing Data have been taken.

It is expected that SRS Data are provided by means of: (i) portable memory devices and (ii) telecommunication lines. In either case, data is transferred outside information systems, etc. for which protection measures are implemented.
Therefore, in order to prevent divulgence, etc. of SRS Data, SRS Instruments Users and SRS Data Holders are required to take measures against physical theft and loss including the lock of containers, in the case of transfer by means of portable memory devices, or to secure secrecy by encryption or other means, in the case of transmission through telecommunication lines. Even if data is obtained by a third party, measures must be taken such that SRS data to be transferred or transmitted may not be viewed.

[Examples of methods]

① Use a lockable container upon the transfer, and store the SRS Data on electronic memory device after encryption, coding and password protection.
② In the case of transmission through telecommunication, encryption of the telecommunication route by SSL (TLS), IPSec, etc. or by using a dedicated line or VPN line.
③ For emails summarizing details of data transmission, transmit an email message encrypted by S/MIME, etc., or attach to an email an encrypted document summarizing details.

(v) that for processing of Satellite Remote Sensing Data, necessary measures have been taken to ensure that such processing is implemented in an appropriate manner.

SRS Data are categorized according to the degree of their processing. In the case where

the processing is incomplete, electronic or magnetic records which would otherwise have been processed into non-SRS Data might be considered as SRS Data. Provision of such data may result in harm to the Ensuring of the Peace of the International Community, etc.
Therefore, SRS Instruments Users and SRS Data Holders are required to establish systems to ensure that appropriate processing are applied according to the relevant categories.

[Examples of methods]

① Clearly specifying the responsible person in charge of processing SRS Data.
② Clearly specifying the person engaged in the business of processing SRS Data.
③ Clearly specifying the procedures for processing SRS Data.
④ Implement the processing according to the prescribed procedures (in the case of automatic processing using a system, take measures such as ensuring that unauthorized persons cannot make modification to the setting)
⑤ Implementing processing at the designated facilities.
⑥ Clearly specifying the purpose of processing SRS Data.

*For research and development for which procedures are not established, ensure that processing is appropriately managed by a supervisor.

■Article 7, paragraph (2) of the Enforcement Regulation
In the case of managing business of handling SRS Data, in whole or in part, by the use of third party storage service provided through telecommunication lines, it is required to take measures equivalent to the safety management measures referred to in Article 7, paragraph (1) under a service contract with a provider of such service, ensure that SRS Data is not stored on a computer located in country with potential risks, and expressly provide for the above measures in the case of subcontracting such business to another party.
The details of the measures are as provided in the Enforcement Regulation.

■Article 7, paragraph (3) of the Enforcement Regulation
For SRS Data provided for the public interest or for the urgent necessity for responding to the need to rescue human lives or other emergencies, requiring the same level of safety management measures as general SRS Data would increase the burden of a holder of SRS Data, leading to a negative impact on service for the public interest and swift disaster response. As such, these safety management measures are not required

for data possessed within the scope necessary to achieve the above objectives.

2.2.4. Preparation and Management of Logs

Article 23 of the Act (Log)

(1) A person who obtained a certification under Article 21, paragraph (1) of the Act must keep a log and record the matters specified by Cabinet Office Order in relation to the status of handling of Satellite Remote Sensing Data, pursuant to the provisions of Cabinet Office Order.

(2) The log under the preceding paragraph must be preserved pursuant to the provisions of Cabinet Office Order.

Article 30 of the Enforcement Regulation (Matters to be Stated in Logs)

(1) The matters specified by Cabinet Office Order, as referred to in Article 23, paragraph (1) of the Act, are as set forth in the following items:

(i) Identification Codes of Satellite Remote Sensing Data for receiving or providing Satellite Remote Sensing Data;

(ii) Categories of Satellite Remote Sensing Data;

(iii) date and time of receiving or providing the Satellite Remote Sensing Data;

(iv) the name of the recipient or provider, and, the certificate number of the recipient or provider if the recipient or provider has obtained a certificate under Article 21, paragraph (4) of the Act; and

(v) status of processing or deleting the Satellite Remote Sensing Data.

(2)When a person who obtained a certification under Article 21, paragraph (1) of the Act creates electronic or magnetic records for the log under Article 23, paragraph (1) of the Act, the person must do so by a method of recording the created electronic or magnetic records on a file stored in a computer used by the person who obtained certification under Article 21, paragraph (1) of the Act, or by a method of preparing the records using Magnetic Disks, etc.

(3) A person who obtained a certification under Article 21, paragraph (1) of the Act must record in the log the matters set forth in the items of paragraph (1) without delay for, each instance of receiving or providing the Satellite Remote Sensing Data, or processing or deleting of Satellite Remote Sensing Data, and must keep the record for five years from the entry of the information.

A person who obtained a certification under Article 21, paragraph (1) of the Act is required to prepare a log to record the status of handling of SRS Data and preserve such log.

More concretely, in relation to the following matters, if there occurs any event which

requires entry of information into the log, the relevant person is required to make such entry without delay and to preserve the log for the designated period.

■Article 30, paragraph (1), items (i) to (iv) of the Enforcement Regulation
Provision of SRS Data to other parties must be made in accordance with the category of such data. In order to verify that the SRS Data is provided in an appropriate manner, it is necessary that the category of data and the name of recipients, in addition to the Identification Codes of the SRS Data and date and time of provision, are recorded in the log.

■Article 30, paragraph (1), item (v) of the Enforcement Regulation
In order to identify the status of SRS Data, it is necessary that the status of the processing and deletion, as well as provision to third parties, is recorded in the log.
More concretely, the relevant person is required to enter into the log the Identification Codes of the SRS Data to be processed and the details of such processing, in the case of processing; or the Identification Codes of the SRS Data to be deleted and the date and time of method of the deletion, in case of deletion.

■Article 30, paragraph (2) of the Enforcement Regulation
Information on handling of SRS Data is generally created and managed on a computer. As such, creation of such information by way of electronic or magnetic records is acceptable.

■Article 30, paragraph (3) of the Enforcement Regulation
In order to verify that the SRS Instruments User is handling the SRS Data in an appropriate manner, it is necessary that each of the activities specified in the Enforcement Regulation are recorded in the log without delay.

3. Review of Guidelines

Details of measures relating to the use of SRS Instruments and treatment of SRS Data are subject to change due to technological development and international situations. These Guidelines will be reviewed as appropriate, according to the change in various circumstances.