

Overview of the Act on the Protection of Specially Designated Secrets (SDS)

Cabinet Secretariat

Preparatory Office for Enforcement of the Act
on the Protection of Specially Designated Secrets

Overview of the Act on SDS Protection: 1. Designation of SDS

Provisional Translation

1. The head of an administrative organ shall designate as Specially Designated Secrets ① information of the types listed in the table below, ② which is kept undisclosed, and ③ which requires special secrecy because unauthorized disclosure thereof would cause severe damage to the national security of Japan.

Item (i) Defense

* Equivalent to the Appended Table 4 of the SDF Law

- (a) Operation of the Self-Defense Forces or thereto relevant assessments, plans or research
- (b) Signal or imagery information, and other important information collected in relation to defense
- (c) Collection and organization of information listed in (b) or the capacity to do so
- (d) Assessments, plans or research pertaining to development of defense capability
- (e) Type or quantity of weapons, ammunition, aircraft and other material for defense use
- (f) Structure of communications network and means of communications for defense use
- (g) Cryptology for defense use
- (h) Specifications, performance or usage of weapons, ammunition, aircraft or other material for defense use including those at the R&D stage
- (i) Methods of production, inspection, repair or examination of weapons, ammunition, aircraft and other material for defense use including those at the R&D stage
- (j) Design, performance or internal use of facilities for defense use

Item (ii) Foreign Affairs

- (a) Among policy or contents of negotiations or cooperation with foreign governments or international organizations, those pertaining to the protection of lives and bodies of people, territorial integrity and other issues deemed important to national security
- (b) Measures including embargoes on imports or exports that Japan carries out for national security purposes or thereto relevant policies
- (c) Important information collected regarding the protection of the lives and bodies of people, territorial integrity, or the peace and security of the international community, or information that requires protection under international agreements including treaties related to national security
- (d) Collection and organization of information listed in (c) or the capacity to do so
- (e) Cryptology for diplomatic use, including communications between the Ministry of Foreign Affairs and Japanese diplomatic establishments

Item (iii) Prevention of Designated Harmful Activities (e.g. Counterintelligence)

- (a) Measures to prevent Designated Harmful Activities or thereto relevant plans or research
- (b) Important information collected on the protection of lives and bodies of people, or information collected from foreign governments or international organizations in relation to prevention of Designated Harmful Activities
- (c) Collection and organization of information listed in (b) or the capacity to do so
- (d) Cryptology used for prevention of Designated Harmful Activities

Item (iv) Prevention of Terrorism

- (a) Measures to prevent terrorism or thereto relevant plans or research
- (b) Important information collected on the protection of lives and bodies of people, or information collected from foreign governments or international organizations in relation to prevention of terrorism
- (c) Collection and organization of information listed in (b) or the capacity to do so
- (d) Cryptology used for prevention of terrorism

2. The head of an administrative organ shall set **the term of designation of up to 5 years (renewable)** and **revoke the designation** before the expiration date as soon as the designated information is found to no longer meet the requirements for designation.
3. The term of designation **shall not exceed 30 years in total** unless the head of the administrative organ obtains **the approval of the Cabinet** by providing compelling reasons for the extension of the term in order to ensure the safety of the state and the people. Even in this case, the head **may not extend the term when it exceeds 60 years in total** except for such cases as involving information on cryptology and human intelligence sources.
4. The head of an administrative organ shall take **necessary measures to protect SDS** including limiting the range of officials who handle SDS and putting classification markings on documents containing SDS.

1. Limitations on Access to SDS

Access to SDS shall be limited to **government personnel, employees of GoJ contractors and prefectural police officers who, following the security clearance process, are identified as not risking unauthorized disclosure of SDS.**

* The heads of administrative organs, Ministers, Deputy Chief Cabinet Secretaries, Special Advisors to the Prime Minister, Senior Vice-Ministers, Parliamentary Secretaries and other executives specified in a Cabinet Order based on their duties, etc. shall be allowed to have access to SDS without undergoing the security clearance process.

** Those receiving SDS for the sake of the public interest (see page 3) shall not be required to undergo the security clearance process.

2. Adjudicators

Heads of administrative organs (or chiefs of prefectural police headquarters)

3. Examinees

Those who are expected to handle SDS in duty among government personnel, employees of GoJ contractors or prefectural police officers

4. Matters for Investigation

- | | |
|--|---|
| (1) Involvement in Designated Harmful Activities and terrorism | (5) Mental health |
| (2) Criminal and disciplinary records | (6) Abuse of alcohol |
| (3) Records of abuse of information | (7) Financial records including credit standing |
| (4) Misuse of drugs and their influence | |

* With respect to investigations regarding (1), the scope of investigation into examinees' relatives (spouses, parents, children and siblings, as well as spouses' parents and children) and cohabitants shall be limited to name, date of birth, nationality and address.

5. Procedures

Obtain examinees' consent

To the extent necessary for the procedures,
(i) Ask questions to the examinees and those concerned including their supervisors and colleagues;
(ii) Request that examinees submit materials;
(iii) Make inquiries with public or private organizations

Determine whether the examinees are deemed at risk of unauthorized disclosure of SDS

Notify the examinees of the results

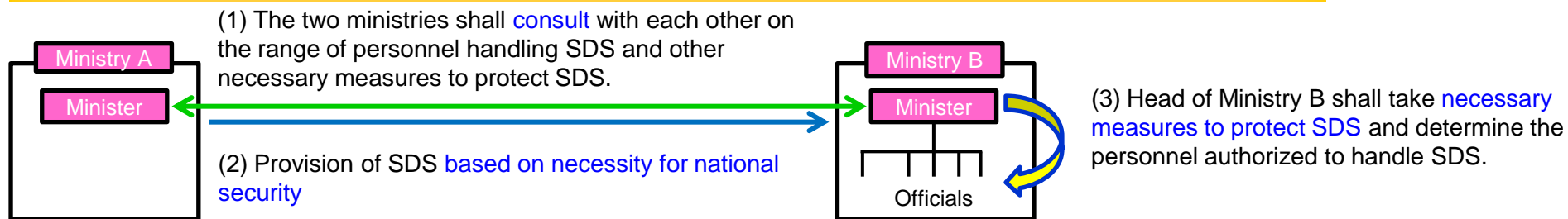
Respond to the examinees' complaints on the procedures

6. Ban on Use and Provision of Information Obtained in the Procedures for Any Other Purposes

- (1) Refusal to undergo the security clearance procedures
- (2) Results of the procedures
- (3) Personal information obtained in the procedures

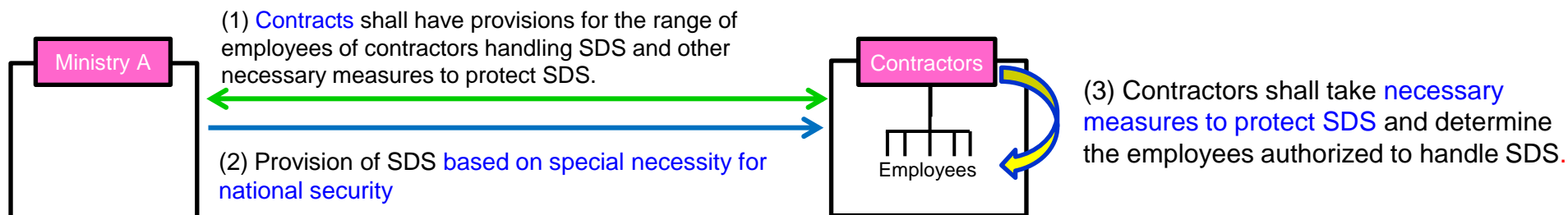
} shall not be **used or provided for any other purposes** except for cases where the examinees are alleged to warrant a disciplinary punishment under the National Public Service Act, etc.

1 Provision of SDS to Other Administrative Organs Based on Necessity for National Security



* The Commissioner-General of the National Police Agency shall, when providing prefectural police with SDS, give instructions to the recipient police on necessary measures to protect SDS.

2 Provision of SDS to GoJ Contractors Based on Special Necessity for National Security



3 Other Cases of SDS Provision for the Sake of the Public Interest

- (1) Provision of SDS to **foreign governments or international organizations where necessary measures to protect SDS are taken**
- (2) Provision of SDS to undisclosed reviews or research by the Diet, criminal investigations and other **activities for the sake of special public interest** on condition that **measures to protect SDS** are taken and that **the head of the providing administrative organ confirms such provision would not cause severe damage to the national security of Japan**
- (3) Presentation of SDS to courts in accordance with Paragraph 6, Article 223 of the Code of Civil Procedure, or to review boards for examinations in accordance with Paragraph 1, Article 9 of the Act on the Establishment of the Information Disclosure and Personal Information Protection Review Board (the so-called “in-camera” procedure)

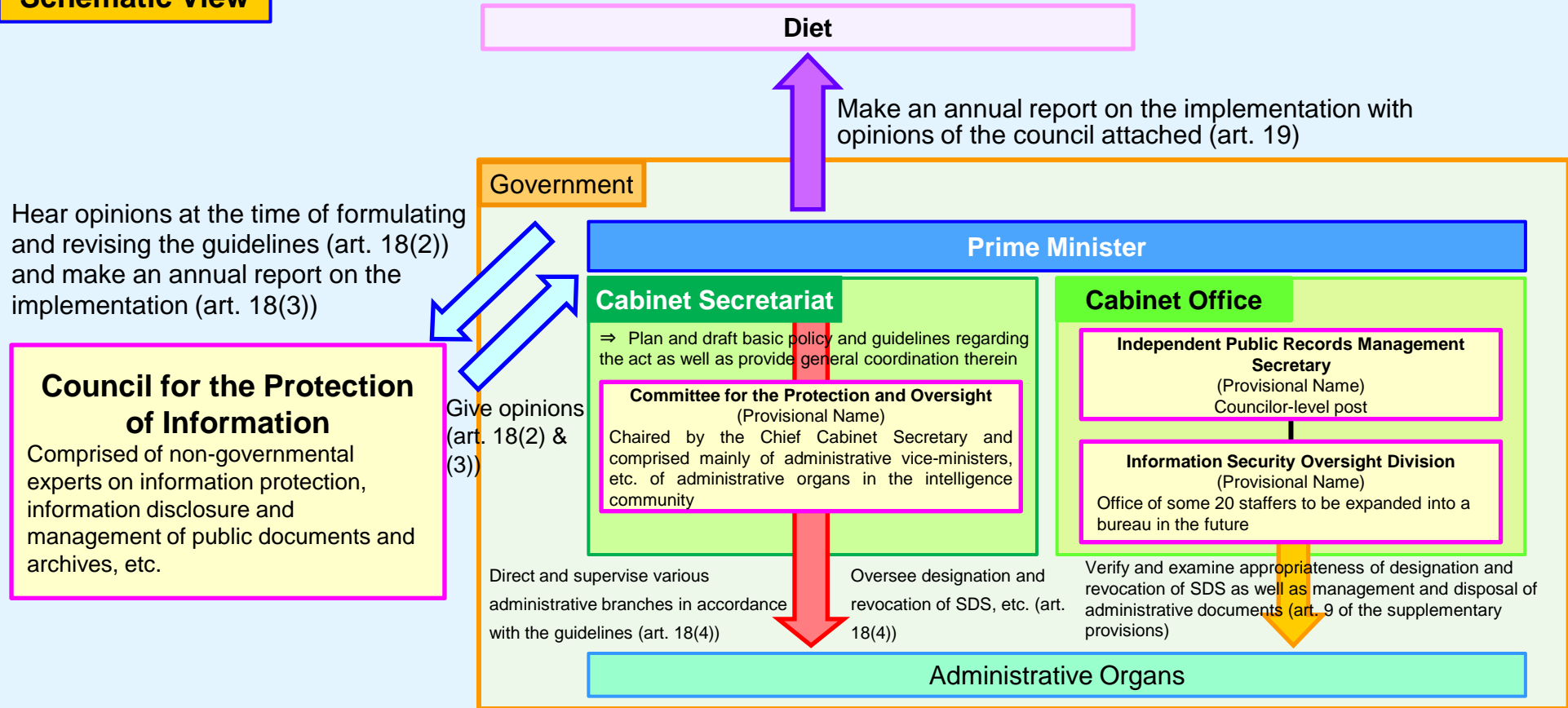
Overview of the Act on SDS Protection: 4. Appropriate Implementation

Provisional Translation

Multilayered System for Appropriate Implementation of the Act

1. **Uniform guidelines** concerning SDS designation, etc. shall be **determined by the Cabinet after taking input from an expert panel** comprised of specialists in the protection of information on national security, information disclosure, management of public documents and archives, etc.
2. **The Prime Minister** may order the head of an administrative organ to **improve the implementation of the act** in accordance with the guidelines.
3. The government shall **submit to the Diet and make publicly available an annual report on the implementation of this act**, with opinions of the expert panel attached to the report.
4. Deliberations will take place to ensure appropriate implementation of the act and necessary steps, including the **establishment of an independent and impartial organ charged with reviewing implementation**, etc., shall be implemented based on the results of these deliberations.

Schematic View



Penalty for Unauthorized Disclosure of SDS, etc.

1. Unauthorized disclosure of SDS shall be punished when **intentionally or negligently** committed by:
 - (1) **Those handling SDS as part of their duties**
Intentional: Imprisonment for **not more than 10 years**
By negligence: Imprisonment for **not more than 2 years** or fine of **not more than 500,000 yen**
 - (2) **Those receiving and thus knowing SDS from an administrative organ for the sake of the public interest**
Intentional: Imprisonment for **not more than 5 years**
By negligence: Imprisonment for **not more than 1 year** or fine of **not more than 300,000 yen**
2. **Acquisition of SDS through the following acts to serve the interests of foreign countries, etc. shall be punished by imprisonment for not more than 10 years:**
 - (1) Fraud, assault or intimidation; (2) Theft; (3) Intrusion on relevant facilities; (4) Eavesdropping on wired telecommunications; (5) Unauthorized access; (6) Any other act excluding (2) to (5) that undermines control of SDS holders.
3. Those who **attempt, conspire to effect, instigate or incite** intentional leakage or acquisition of SDS through the acts listed above shall be punished.

Other Issues including Interpretation and Application of This Act

1. The act stipulates that **stretching the interpretation of the act to unduly infringe on the fundamental human rights of the citizens shall be prohibited**, and that **due consideration be given to freedom of the press and news gathering that contributes to guaranteeing the people's right to know**.
2. The act also stipulates that **news gathering by those engaged in publishing and the press shall be lawful as long as it is intended exclusively to serve the public interest and is not judged to be done through violations of laws or grossly unreasonable means**.
3. The act shall take effect within 1 year of its promulgation and stipulate transitional measures regarding limiting the range of SDS handlers.
4. The Self-Defense Forces Law shall be partially revised to delete provisions for Defense Secrets (*Bouei Himitsu*).
5. The Cabinet Act shall be partially revised so that **the Director of Cabinet Intelligence shall administer the affairs of protection of Specially Designated Secrets**.