Appendix 1

Criteria for Evaluating the Impact of Operations and Information Related to the Use of SaaS

The original texts of the Standards are prepared in the Japanese language, and these translations are to be used solely as reference material to aid in the understanding of the Standards.
For all purposes of interpreting and applying the Standards in practice, users should consult the original Japanese texts available on the following website:
https://www.ismap.go.jp/csm

1. General Provisions

Based on Chapter 5 of these Rules, the information related to each business handled and processed by SaaS is evaluated to determine the impact if any of the confidentiality, integrity, and availability defined in the Common Standards for Cybersecurity Measures at Governmental Agencies and Related Agencies (established by the Cybersecurity Strategic Headquarters on July 7, 2021) is compromised. The impact for each type of operations and information is evaluated as low, moderate, or high.

2. Viewpoints for Evaluating the Impact of Operations and Information

The Risks Envisioned for SaaS Usage (1) to (6) are the basic viewpoints for evaluating the impact. The Risks Envisioned for SaaS Usage are set in reference to the "Risks Envisioned for Online Procedures" listed in the Compliance Rule 6.1.1(1)(b) in Chapter 6 of the Guidelines for Formulating Countermeasure Criteria for Government Agencies (2021 version), and based on the assumption that the SaaS, due to its properties, is to be mainly used for tasks within government agencies.

Risks Envisioned for SaaS Usage

① Inconvenience, distress, or damage to standing or reputation
② Financial loss (for example, causes monetary damage or liability to the user)
③ Harm to agency programs or public interests
④ Unauthorized release of sensitive information (personal information, etc.)
⑤ Personal safety
⑥ Civil or criminal violations

3. Impacts per Category

This section defines the potential impacts for each category of harm based on the properties of SaaS, in reference to Appendix A "7. Calculating Impact for Each Type of Risk" in the Guidelines for Online Identity Verification Methods in Administrative Procedures.

Government agencies, etc., are required to evaluate the impact for information related to their operations, in consideration of the impact of category. A result of N/A is possible when evaluating the impact for information related to various types of operations. However, for the result of the whole series of evaluations related to the operations handled by SaaS (defined as the "Overall Evaluation"), the evaluation must be made in the three stages of "low," "moderate," or "high."

Potential impact of “1. Inconvenience, distress, or damage to standing or reputation”

Level	Contents
N/A	No risk (not envisioned).
Low	At worst, limited, short-term inconvenience, distress, or embarrassment to any party.
Moderate	At worst, serious short-term or limited long-term inconvenience, distress, or damage to the standing or reputation of any party.
High	Severe or serious long-term inconvenience, distress, or damage to the standing or reputation of any party. This is ordinarily reserved for situations with particularly severe effects or which potentially affect many individuals.

Potential impact of “2. Financial loss (for example, causes monetary damage or liability to the user)”

Level	Contents
N/A	No risk (not envisioned).
Low	At worst, an insignificant or inconsequential financial loss to any party, or at worst, an insignificant or inconsequential agency liability.
Moderate	At worst, a serious financial loss to any party, or a serious agency liability.
High	Severe or catastrophic financial loss to any party, or severe or catastrophic agency liability.

Potential impact of “3. Harm to agency programs or public interests”

Level	Contents
N/A	No risk (not envisioned).
Low	At worst, a limited adverse effect on organizational operations or assets, or public interests. Examples of limited adverse effects are: (i) Mission capability degradation to the extent and duration that the organization is able to perform its primary functions with noticeably reduced effectiveness. (ii) Minor damage to organizational assets or public interests.
Moderate	At worst, a serious adverse effect on organizational operations or assets, or public interests. Examples of serious adverse effects are: (i) Significant mission capability degradation to the extent and duration that the organization is able to perform its primary functions with significantly reduced effectiveness. (ii) Significant damage to organizational assets or public interests.
High	A severe or catastrophic adverse effect on organizational operations or assets, or public interests. Examples of severe or catastrophic effects are: (i) Severe mission capability degradation or loss of to the extent and duration that the organization is

	unable to perform one or more of its primary functions (ii) Major damage to organizational assets or public interests.

Potential impact of “4. Unauthorized release of sensitive information (personal information, etc.)”

Level	Contents
N/A	No risk (not envisioned).
Low	At worst, a limited release of personal, government sensitive, or commercially sensitive information to unauthorized parties resulting in a loss of confidentiality with a limited adverse impact on the activities or assets of agencies, etc., or on the user.
Moderate	At worst, a release of personal, government sensitive, or commercially sensitive information to unauthorized parties resulting in loss of confidentiality with a significant adverse impact on the activities or assets of agencies, etc., or on the user.
High	A release of personal, government sensitive, or commercially sensitive information to unauthorized parties resulting in loss of confidentiality with a catastrophic or devastating impact on the activities or assets of agencies, etc., or on the user.

Potential impact to “5. Personal safety”

Level	Contents
N/A	No risk (not envisioned).
Low	At worst, minor injury not requiring medical treatment.
Moderate	At worst, moderate risk of minor injury or limited risk of injury requiring medical treatment.
High	A risk of serious injury or death.

Potential impact of “6. Civil or criminal violations”

Level	Contents
N/A	No risk (not envisioned).
Low	At worst, a risk of civil or criminal violations of a nature that would not ordinarily be subject to enforcement efforts.
Moderate	At worst, a risk of civil or criminal violations that may be subject to enforcement efforts.
High	A risk of civil or criminal violations that are of special importance to enforcement programs.