ITSP.10.033 STARTER TEMPLATE · SoS

Statement of Sensitivity

Categorization and injury assessment worksheet aligned to ITSG-33 and ITSP.10.033

Harry Foy

EDITION 1.0 · 2026

Statement of Sensitivity

Categorization and injury assessment worksheet aligned to ITSG-33 and ITSP.10.033

EDITION 1.0 · 2026

Harry Foy

Skymeba Cybersecurity Solutions

Calgary, Canada

STARTER TEMPLATE — CUSTOMIZE FOR YOUR SYSTEM

Every heading, prompt, and field in this template is intended to be replaced, expanded, or removed to match the system being assessed. Italic text in muted grey is placeholder guidance for the author.

How to use this template

The Statement of Sensitivity (SoS) is the first artifact in a Government of Canada Security Assessment & Authorization package. It records what information the system holds, how sensitive that information is, and the injury the department would suffer if confidentiality, integrity, or availability were lost. Everything downstream — the control profile, the SSP, the TRA, and ultimately the ATO — anchors back to this document.

This starter template mirrors the ITSG-33 SoS structure and the ITSP.10.033 categorization vocabulary. Complete every field in order; do not skip §3 (information types) — it is the source of truth for §4 (aggregate categorization). Italic muted text is guidance for the author and should be replaced.

Have the business owner and the departmental privacy officer sign the completed SoS before drafting the SRTM. An unsigned SoS is a common cause of rework: assessors will re-open scope if the categorization was never formally accepted.

1 · System identification

One-page snapshot the recipient DSO can read in 60 seconds.

System name

[Full name of the system as approved by the business owner.]

System acronym / identifier

[Short identifier used in tickets, dashboards, and CMDB.]

Business owner

[Name, title, department. This is the accountable executive.]

System owner / delegate

[Name, title. Day-to-day authority for the system.]

Departmental Security Officer (DSO)

[Name, title. Signs the ATO under delegated authority.]

Security Assessment lead

[Name, firm, contact. May be internal or contracted.]

Assessment scope version

[e.g. Initial ATO, Reassessment, Change scope. Include date.]

2 · Business context

Capture the mission the system supports, the users it serves, and the legislative or programmatic drivers behind its operation. This is the record the DSO returns to when weighing residual risk against business need.

Mission or program

[What government service or program does this system deliver?]

User populations

[Public, employees, other departments, industry — with rough counts.]

Business hours / criticality

[24×7, business-hours only, seasonal peaks. Any hard availability commitments?]

Legislative or regulatory drivers

[Privacy Act, PIPEDA, Access to Information, sector-specific law.]

Related programs / dependencies

[Systems this SoS depends on or feeds. Cite by SA&A id where possible.]

3 · Information types held or processed

Enumerate each information type separately. If aggregated, note the aggregation and its uplift to categorization.

Information type	Description	Handling / release
[e.g. Client benefit records]	[Personal information subject to Privacy Act; captured through service delivery.]	[Protected B; disclosure only via ATIP or by consent.]

3.1 Confidentiality / Integrity / Availability by type

Rate each information type separately, then justify the aggregate below.

Type	C	I	A	Rationale (injury statement)
[Type 1]	L/M/H	L/M/H	L/M/H	[Concise injury statement anchoring the rating.]

C = Confidentiality · I = Integrity · A = Availability. Use L (Low), M (Medium), or H (High).

4 · Aggregate categorization

The system inherits the highest categorization across its information types unless a defensible tailoring is documented here. Justify any downgrade in writing and record who approved the departure from default aggregation.

Aggregate confidentiality	*[Protected A / B / C / Classified]*
Aggregate integrity	*[Low / Medium / High]*
Aggregate availability	*[Low / Medium / High]*
Overall impact level	*[Low / Medium / High — the level used for control selection.]*
Cloud profile (if applicable)	*[CCCS Medium, PB PBMM cloud, on-prem-only, etc.]*

5 · Injury assessment

The injury statements below drive the categorization. Write each one as an outcome sentence: who is injured, how, and to what degree.

Injury from loss of confidentiality

[e.g. Disclosure would cause serious injury to individuals identified in the benefit record and moderate embarrassment to the Government of Canada.]

Injury from loss of integrity

[e.g. Unauthorized alteration would misdirect benefit payments and require months of remediation.]

Injury from loss of availability

[e.g. A 24-hour outage would delay statutory decisions and generate ministerial correspondence.]

Cumulative or cross-system injury

[Injury arising from aggregation with other systems or programs; cite the systems by name.]

6 · Special categories of information

Note whether any of the following apply. Each triggers extra obligations beyond the base categorization.

- **Personal information (PI)** — obligations under the Privacy Act; PIA may be required.
- **Sensitive personal information** — health, biometrics, sexual orientation, ethnic origin.
- **Third-party or commercial confidence** — solicitation, negotiations, tenders.
- **Cabinet confidences / advice to minister** — additional handling under s. 69 of the ATIA.
- **Law-enforcement or investigative records** — distinct release regime.

- **International or shared-with-allies information** — treaty obligations may apply.

7 · Downstream artifact map

Record how this SoS is used to derive later SA&A artifacts. Assessors will trace back from every finding to a decision originally made here.

Artifact	Decision anchored here	Owner
Security Control Profile / SRTM	[Which control profile applies — CCCS Medium, TBS Protected B, custom.]	[Security architect.]
System Security Plan (SSP)	[Boundary and control implementation scoped to the info types listed here.]	[System owner.]
Threat and Risk Assessment (TRA)	[Threat scenarios weighted by the injury statements in §5.]	[TRA lead.]
Privacy Impact Assessment (PIA)	[Triggered if §6 flags personal information.]	[Departmental privacy officer.]

Approvals

The signatures below confirm that the responsible parties have reviewed this document, that its contents accurately reflect the system, and that the recorded decisions are authorized.

Business owner

Accountable for the mission the system supports and for accepting the categorization recorded here.

Name	Signature	Date

System owner / delegate

Day-to-day authority for the system; confirms that the categorization matches operational reality.

Name	Signature	Date

Departmental Security Officer (DSO)

Confirms the SoS supports the SA&A path selected for this system.

Name	Signature	Date

Departmental Privacy Officer

Required signature when personal information is in scope; confirms PIA status.

Name	Signature	Date