# Declassifying Intelligence

April 2023



Government of Canada
Privy Council Office
Gouvernement du Canada
Bureau du Conseil privé

Canada

# Overview

- Why We Classify?
- Declassification
- Considerations in Declassification: The Balancing Act
- Canadian Legal and Policy Framework
  - Safeguarding
  - Disclosure
- Current Realities
- Policy Renewal
- PCO's Role
- Case Study: Declassification

# Why We Classify?

To protect information or assets that, if compromised, could be expected to cause injury to:

- Human sources, confidential informants, covert officers and protected persons;
- Intelligence techniques and tradecraft, including technical sources;
- Allied intelligence equities and information shared in confidence;
- Military plans, capabilities, techniques, and equipment;
- Encryption and cryptographic systems;
- International relationships and partnerships;
- Canada's reputation as a trusted partner; and,
- Etc.

# Declassification

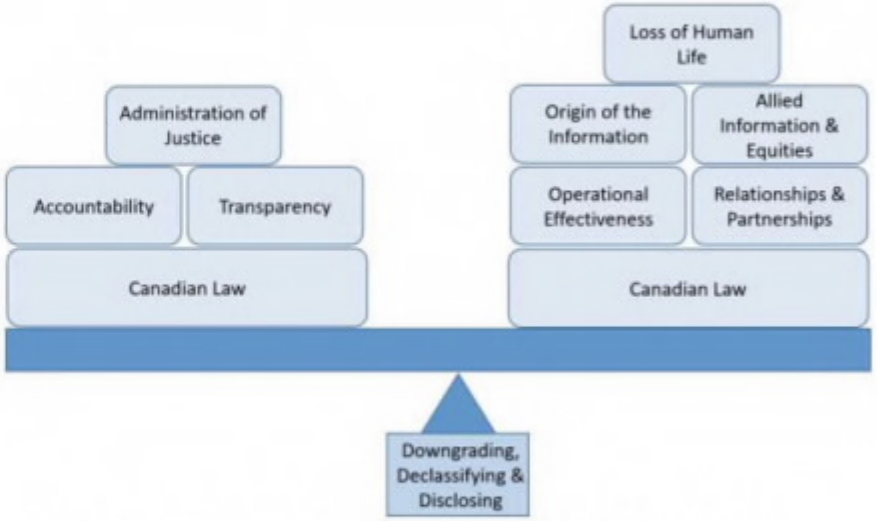
**Declassification:**

- When the disclosure of classified information is no longer considered to be injurious to the national interest, the information can be declassified.
- The classification level of the information is therefore downgraded to a lower classification or unclassified all together.
- There is no formal proactive declassification policy across the Government of Canada. Canada remains the only Five Eyes country without a formal declassification strategy.
- Examples of documents being declassified for disclosure include:
  - The release of documents under *Access to Information Act;*
  - The review and release of documents in response to foreign partner declassification requests; and/or,
  - Decisions by the Government of Canada to review a specific matter for declassification in the public interest.

# The Balancing Act

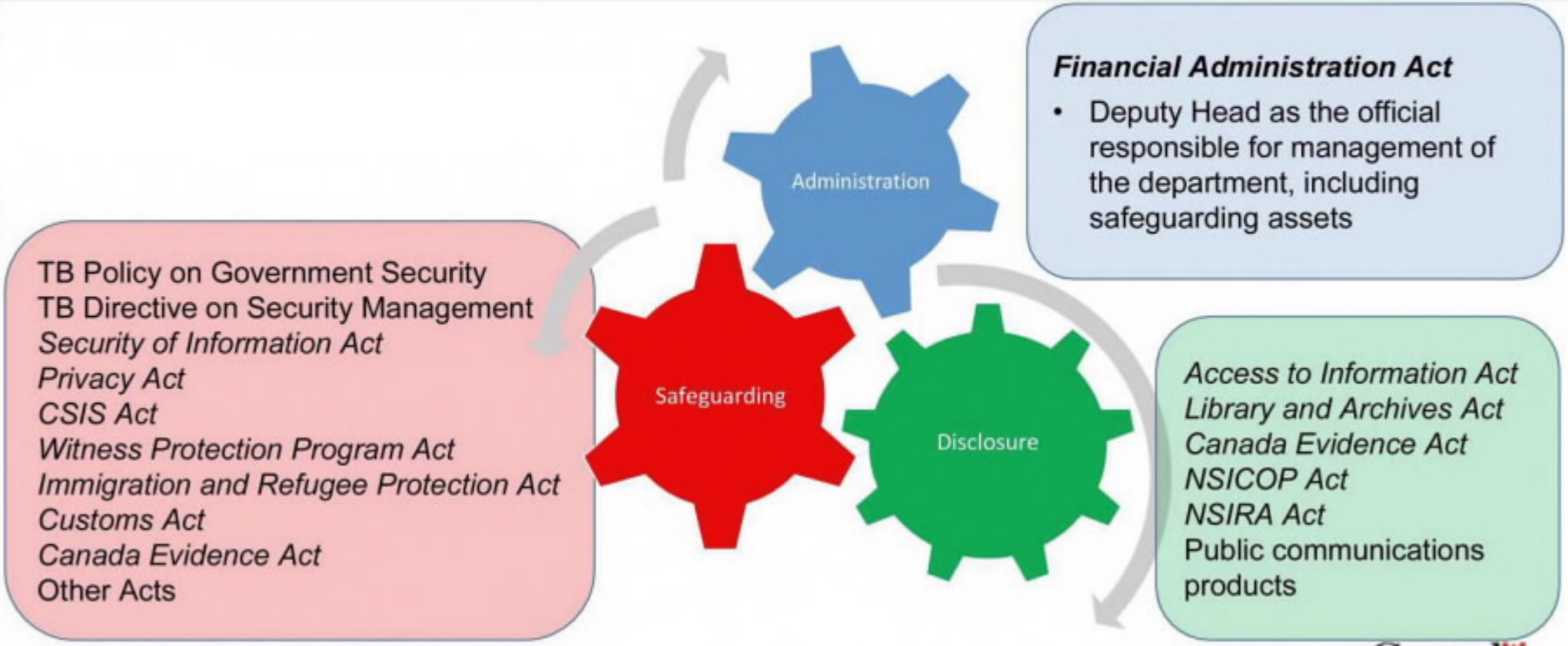
When disclosing national security information and intelligence, it is a balancing act that takes into account:

- public interest in accountability, transparency and administration of justice;
- Canadian laws, including the *Privacy Act;*
- originator control restrictions;
- potential loss of human life (human sources, covert officers, confidential informants and protected persons);
- effectiveness of ongoing and future operations (sources, tradecraft, techniques, encryption and cryptographic systems and military plans and capabilities);
- impact on international and domestic relationships and partnerships; and,
- potential impact on future access to sensitive allied information and equities.




**The Originator of the information controls the classification of that information and is solely responsible for deciding if/when it can be declassified.**

# Legal & Policy Frameworks




***Financial Administration Act***

- Deputy Head as the official responsible for management of the department, including safeguarding assets

TB Policy on Government Security
TB Directive on Security Management
*Security of Information Act*
*Privacy Act*
*CSIS Act*
*Witness Protection Program Act*
*Immigration and Refugee Protection Act*
*Customs Act*
*Canada Evidence Act*
Other Acts

*Access to Information Act*
*Library and Archives Act*
*Canada Evidence Act*
*NSICOP Act*
*NSIRA Act*
Public communications products

# Policy Frameworks: Safeguarding

**TB Policy on Government Security**

- Deputy Head responsible for classification and declassification.

**Directive on Security Management**

- Time frame for protection should be as short as possible.
- Departments must adhere to legal, policy and privacy considerations; the principle of originator control; and, international and domestic agreements.
- Officials should assess for injury.

# Legal Frameworks: Safeguarding

***Security of Information Act***

- Makes it an offence to reveal 'special operational information'.

***Privacy Act***

- Prohibits disclosure of personal information without consent or authority.

***Canada Evidence Act***

- Sets out a process for the protection of sensitive and injurious information during a proceeding; balanced against public interest of disclosure given the nature of the proceeding.

**Other Acts**

- Protect national security information from being disclosed during legal proceedings.

# Legal Frameworks: Safeguarding

## Department Specific

***CSIS Act***

- Prevents disclosure of information relating to CSIS activities, e.g. concerning a human source.

***Witness Protection Program Act***

- Prevents disclosure of information concerning protected persons and methods of protection.

***Immigration and Refugee Protection Act (IRPA)***

- Defines measures to protect information that could be injurious to national security or endanger the safety of any person.

***Customs Act***

- Prohibits the disclosure of customs information without proper authorization.

# Legal & Policy Frameworks: Disclosure

## Declassification

***Access to Information Act (ATIA)***

- Public has a right to access records.
- No proactive disclosure of historical records.
- Proscribes exceptions and exclusions to access.
- Application of exceptions should be limited and specific.

***Library and Archives Act***

- Historical records are accessible once archived; classified ones are not accessible except via *ATIA*.

***Canada Evidence Act***

- Under s. 38 of the *CEA*, the Federal Court may authorize the disclosure of otherwise injurious information if it determines that the public interest in disclosure outweighs the public interest in non-disclosure.

# Legal & Policy Frameworks: Disclosure

## Publication

***NSICOP Act***

- The NSICOP Act requires the tabling in Parliament of its special reports and an annual public report that summarizes its activities from the previous year.
- The Prime Minister may direct NSICOP to revise a report if it contains specified classes of injurious information.

***NSIRA Act***

- The NSIRA Act requires the tabling in Parliament of an annual public report that summarizes its activities rom the previous year.
- The Deputy Head of the responsible department must be consulted on the report to ensure non-disclosure of injurious information before it is published.

# Legal & Policy Frameworks: Disclosure

## Publication

***CSIS Act***

- The CSIS Act requires the tabling in Parliament of an annual public report that summarizes its activities from the previous year.

***CSE Act***

- The CSE Act requires the department to publish an annual report on its activities each year.

**TBS Directive on the Management of Communications**

- Departments are responsible for working proactively with the media to promote public awareness and understanding of government activities.

**Direction from Cabinet**

- Some Cabinet decisions include explicit direction for public disclosure, reporting or other communications and awareness activities.

# Current Realities: Triggers for Disclosures

- **Disclosure through the *ATIA***
  - When a request is received through the *ATIA*.
- **Request for declassification from a domestic or foreign partner**
  - When a domestic or foreign partner contacts the originating department to request the declassification of records.
- **Government of Canada direction**
  - The Government of Canada issues clear direction that information should be reviewed for declassification or publication.
  - Examples include the publication of CSIS's threat assessments, ITAC threat assessments, and CSE's cyber threat assessments, alerts and advisories.
- **Litigation**
  - When there is an ongoing criminal, civil or administrative proceeding that requires the disclosure of Government of Canada information.
- There is currently **no proactive disclosure** review based on the historical nature of the information.

# Current Realities: Trends and Impacts

Trends:

- General tendency toward over classification.
- Inconsistency by people and organizations in the application of the *ATIA* and declassification requests.
- Very little proactive declassification or release.
- Minimal to no resources to begin proactive declassification.
- The originator of the information owns and decides the classification.

Impacts:

- Limited physical storage space that is expensive to maintain.
- Creates tension in international relationships as responding to declassification requests can be time consuming and disclosure may not be possible.
- Reduces transparency of national security and intelligence activities.
- Reduces public trust and confidence as there are limited means for the national security and intelligence community to highlight past successes or lessons learned.

# Policy Renewal

**Treasury Board Secretariat (TBS)**

- Reviewing the *ATIA* to inform potential reform needed to improve ATI system and address the current backlog.
- TBS is currently considering a Memorandum to Cabinet (MC) for departmental declassification funding.

**Public Safety Canada**

- Developed a National Security & Intelligence Declassification Framework (pilot project from October 2021 to June 2022). Departments are currently reviewing whether the report produced at the conclusion of the pilot project is within the scope initially identified by PS, and whether the methodology and findings support the declassification recommendations made.
- Leads a working group with members from the national security and intelligence community to discuss and engage on issues related to declassification.

**Proactive Disclosures or Foreign and Domestic Partner Declassification Requests**

- In the absence of a formal Government of Canada policy, departments have developed their own *ad hoc* system based on their unique requirements.

# PCO Role

- Advise the Prime Minister, other PCO portfolio Ministers and Cabinet on issues related to disclosure and declassification.
- Lead the discussion with foreign partners on the process related to declassification requests.
- Coordinate the S&I Community when requests implicate multiple departments.
- Where Government of Canada indicates a desire to proactively declassify or write to release intelligence products, PCO helps to coordinate the:
  - Execution
  - Coordination
  - Consistency of messaging
- Assist in advancing a Government of Canada position related to declassification and publication of national security and intelligence information and products.

# Case Study: Declassification

- The US requested, via operational and then diplomatic channels, the declassification of Canadian information provided to the US as part of the investigation of 9/11.
  - This was further to an executive order signed in September 2021 to declassify US records relating to the investigation of 9/11.
  - A more general executive order signed in 2009 prescribes the US system for classifying, safeguarding, and declassifying national security information.
- The purpose of the request was to release the declassified information in the US Court system to support a civil litigation by the victims' families.
- While the initial requests to declassify were sent as per normal practice from intelligence agency to intelligence agency, or law enforcement agency to law enforcement agency, the diplomatic channel became involved and began re-sending requests to intelligence/law enforcement agencies.
- Government of Canada departments provided responses to the various US requests and explained that in most cases they could not declassify the records.
- Important lessons learned for both nations have come out of this process and follow-on work to improve the way requests are sent and managed is underway.

Protected B

# Case Study: Declassification

- In 2021, [redacted] CSE declassify intelligence related to the SolarWinds cyber attack and for Canada to participate in an international effort to publicly attribute the attack to Russia.
- The request was sent directly to CSE for consideration.
  - This Agency-to-Agency action followed standard practice for submitting declassification requests.
- CSE reviewed the material and equities, assessed the injury if released, and weighed the public interest in disclosing.
- After consideration, the Chief of CSE decided to declassify and disclose pieces of information to support the public attribution.
- Global Affairs Canada (GAC), which is the lead department for public attributions, issued a press release supporting the international effort.
- The public release identifies APT29, also named “The Dukes” or “Cozy Bear” as being responsible for the activity and indicates that the individual operates as part of Russian Intelligence Services.