


Protected B


For Public Release


# Declassifying Intelligence

Presentation to the Clerk of the Privy Council Office  
April 2022



 Government of Canada  
Privy Council Office

 Gouvernement du Canada  
Bureau du Conseil privé

Canada 

Protected B

# Overview

- Why We Classify?
- Considerations In Declassification: The Balancing Act
- Canadian Legal and Policy Framework
- Realities
- Policy Renewal
- Recent Case Study
- Former Case Study

For Public Release

Protected B

# Why We Classify?

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

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

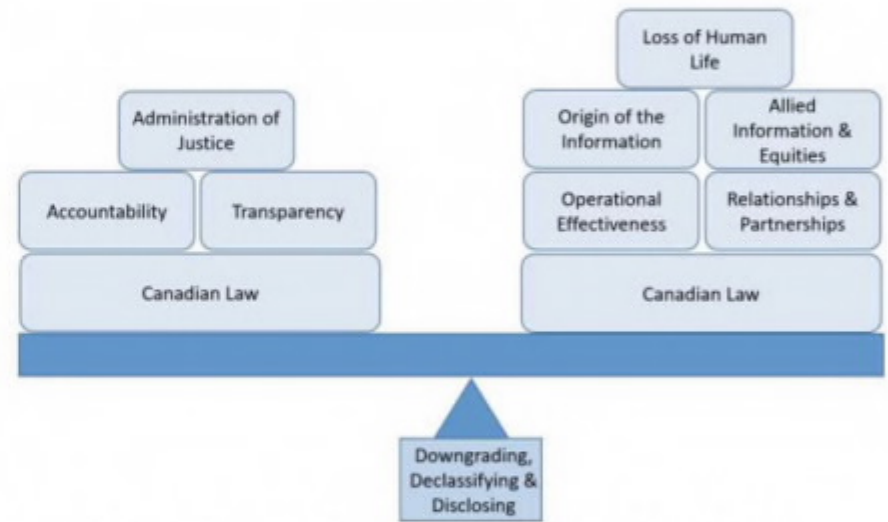
For Public Release

Protected B

# The Balancing Act

When declassifying intelligence, it is a balancing act that takes into account:

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

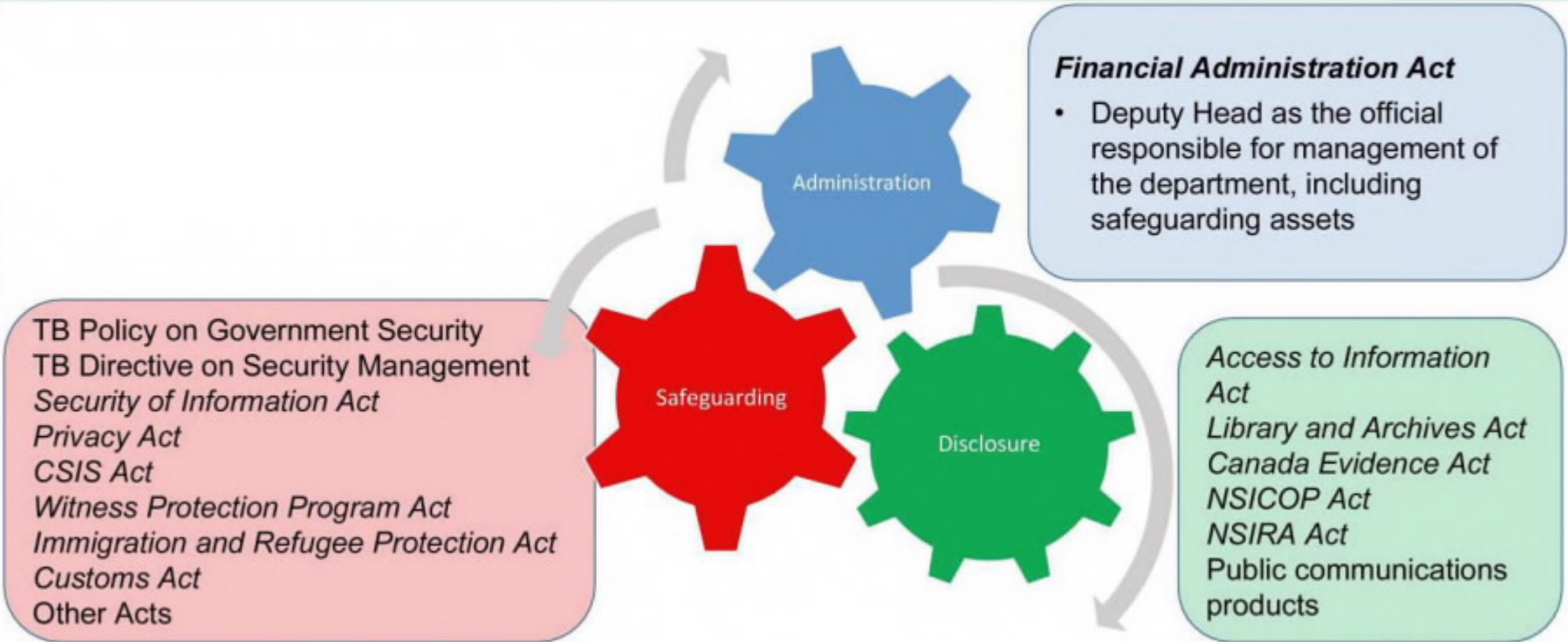


**The Originator of the information controls the classification of that information and is solely responsible for deciding if/when it can be declassified.**

For Public Release

Protected B

# Legal & Policy Frameworks



For Public Release



Protected B

# Legal & Policy Frameworks: Safeguarding

## **TB Policy on Government Security**

- Deputy Head responsible for classification & declassification.

## **Directive on Security Management**

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

## ***Security of Information Act***

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

## ***Privacy Act***

- Prohibits disclosure of personal information without consent or authority.

For Public Release

Protected B

# Legal & Policy Frameworks: Safeguarding Department Specific

### **CSIS Act**

- Prevents disclosure of info concerning a human source.

### **Witness Protection Program Act**

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

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

- Defines measures to implement to protect info that could be injurious to NS or endanger the safety of any person.

### **Customs Act**

- Prohibits the disclosure of customs info without proper authorization.

**Other Acts** protect NS info from being disclosed during legal proceedings.

For Public Release

Protected B

# Legal & Policy Frameworks: Disclosure

## ***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***

- Prohibits individuals from disclosing sensitive or injurious information during a proceeding; balanced again public interest of disclosure given nature of the proceeding.

For Public Release



Protected B

# Legal & Policy Frameworks: Disclosure

## ***NSCIOP Act***

- The Prime Minister may direct NSICOP to revise their report if it contains specified classes of injurious information.

## ***NSIRA Act***

- NSIRA reports are redacted by departments to remove injurious information.

For Public Release

Protected B

# Legal & Policy Frameworks: Disclosure

## Department Specific

### Annual Reports

- Provide aggregated information on the activities and threats identified by departments.

### Communication Releases

- Provide more specific information on department activities related to an issue.

### Conferences and Public Speaking Events

- Senior officials highlight the work of departments and provide information related to threat assessments.

For Public Release

Protected B

## Current Realities

- General tendency toward over classification.
- Inconsistency by people & organizations in the application of the *ATIA* & declassification requests.
- Very little proactive declassification or release.
- Minimal to no resources to begin proactive declassification.
- The originator of the information owns & 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 & disclosure may not be possible.
- Reduces transparency of national security & intelligence activities.
- Reduces public trust & confidence as there are limited means for the national security & intelligence community to highlight past successes or lessons learned.

For Public Release

Protected B

# Policy Renewal

- Public Safety Canada
  - Developed a National Security & Intelligence Declassification Framework (pilot project until June 2022);
  - Leads a working group with members from the national security & intelligence community to discuss & engage on issues related to declassification.
- Treasury Board Secretariat
  - Reviewing the *ATI Act* to inform potential reform needed to improve ATI system & address the current backlog.

For Public Release

Protected B

## Recent Case Study

- 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.

For Public Release



Protected B

## Exemption Criteria

- The US executive orders have two noteworthy exceptions for the Government of Canada to consider related to declassification of information. Information does not need to be declassified if:
  - It reveals foreign government information that would cause serious harm to the relationship with that country if released;
  - It violates an international agreement (e.g. the principle of originator control) and does not permit the automatic or unilateral declassification of information.
- The use of such exemptions by the originator and holder of the information being requested to be declassified should apply such exemptions carefully and not over-broadly.

For Public Release

Protected B

# Former Case Study

- In 2021, the [redacted] CSE declassify intelligence related to the SolarWinds cyber attack & 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, Chief 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 & indicates that the individual operates as part of Russian Intelligence Services.

For Public Release

Protected B

## Annexe: Five Eyes Declassification Comparison

	Responsibility	Exemptions	Oversight/Review
UK	-Each individual agency and department to identify records of historical value.	-Content exempted from release remains at the originating agency and is not sent to the National Archives.	-Secretary of State for Culture, Media and Sport has the power to suspend the release of records for national security reasons. -Secretary of State's Advisory Council on National Records and Archives reviews these decisions.
USA	-Each individual agency and department to identify records for declassification.	-Content exempted from release is reviewed by Interagency Security Classified Appeals Panel (ISCAP)	-Interagency Security Classified Appeals Panel (ISCAP) -Information Security Oversight Office (ISOO)
New Zealand	-Each individual agency and department to identify records and downgrade classification status to "open access" (unclassified).	-Content exempted from release remains at the originating agency and is not sent to the National Archives. -Prime Minister or the Attorney General can recommend non-disclosure if information falls under exemption categories.	-Ombudsman
Australia	-Identification and publication authorities are sole responsibility of the National Archives and Chief Archivist. -Declassification review can be done in consultation with departments and agencies.	-Content exempted from release is determined by National Archives of Australia.	-Administrative Appeals Tribunal

16

## Slide Notes

### Slide 3:

#### National Interest

The Policy on Government Security defines “national interest” as “the security and the social, political and economic stability of Canada.”

### Slide 4:

There is a need to balance the requirement for public interest in transparency, accountability, and administration of justice with classification requirements to limit the disclosure of information that could reasonably be expected to cause injury to the national interest (relating to national security, national defence, and international relations).

Examples include:

#### Ongoing Law Enforcement Investigations

Information relating to ongoing law enforcement investigations, if compromised, could damage or impact the ongoing investigation and subsequent prosecution.

Information that would reveal highly classified or protected information

Example 1: Human or confidential source identities, or individuals in witness protection and the means used to protect them. This information if compromised could lead to the grave bodily harm or loss of human life.

Example 2: Diplomatic correspondence, negotiating positions in relation to international agreements, or assessments of foreign entities.

#### Origin of the Intelligence

Principle of originator control: When information is received in confidence from a foreign or domestic partner, that partner needs to consent to the information could be downgraded, declassified, or disclosed.

Caveats: Information received from partners often contain caveats which explain how the information can be used and when it is important to return to the originator to request for new authorities in using the information.

#### Special Operational Information

Example 1: Military plans, capabilities or limitations

Example 2: Intelligence targets

Example 3: Information that reveals sensitive methods, techniques or sources of intelligence collection, processing, analysis, dissemination or protection (e.g. encryption)

Information protected by the Privacy Act

An individual's personal information, as defined by the Privacy Act, cannot be disclosed without consent or proper authorization.

Once information has been declassified or disclosed in the public interest, it remains declassified for other purposes.

**Slide 5:**

The types of information that could reasonably be expected to cause injury are enshrined in Canadian Legislation and Federal Government Policy. This slide highlights the legal and policy frameworks that define and legislate safeguarding requirements. It also highlights those pieces of legislation that aim to provide the public with access to federal government information albeit with exceptions to ensure safeguarding when needed.

Administration:

Financial Administration Act-

The Financial Administration Act, sets out the Administrative requirements and the delegated authorities for the management of Federal Government Departments. The FAA establishes the Deputy Head as the senior official responsible for the management of the department or agency.

**Slide 6:**

With respect to Safeguarding:

Treasury Board Policies:

In moving on to the 2nd Gear, these policies and Acts relate to the safeguarding of information.



TBS Policy of Government Security governs the classification and declassification of government records. However, it does not contain explicit guidance for the declassification of national security and intelligence records.

The Deputy Head of a department is responsible for implementing the Policy on Government Security and for establishing the department's security governance, including responsibilities for security controls and authorities for security risk management decisions. This includes for the declassification, downgrading, or disclosure of records.

Directive on Security Management aims to achieve efficient, effective, and accountable management of security within departments and agencies.

Within the Appendix E: Mandatory Procedures for Information Management Security Control the directive establishes the need to ensure that the time frame for protection of information is kept as short as possible and that the security category continues to reflect the potential impacts of a compromise: specifically, in relation to downgrading the security classification of information.

Importantly, when downgrading classification, this directive requires that the departments adhere to:

- legal, policy, and privacy considerations;
- the principle of originator control; and,
- any agreements and memoranda of understanding received from other governments of the private sector.

Similarly, Appendix J: Standard on Security Categorization outlines the security categorization process, and defines the need for officials to examine separately the potential for injury that results from a loss of confidentiality, integrity or availability.

Further, the security category determines, in part, security requirements and the need to balance the risk of injury against the cost of applying safeguards throughout the life cycle of information, assets, facilities or services.

Security of Information Act outlines the wrongful communication of classified information or documents as an offence. It stipulates what is considered "special operational information" as information that the Government of Canada is taking measures to safeguard that reveals, or from which may be inferred,

- (a) a confidential source of information, intelligence or assistance to the Government of Canada;
- (b) military operations in respect of a potential, imminent or present armed conflict;
- (c) information about covert collection techniques;
- (d) the object of a covert investigation;

(e) the identity of any person engaged in covert activity;

Privacy Act is intended to protect the privacy of individuals with respect to their personal information held by the government. Within it, the Act requires that a disclosure will not affect any person's privacy interest more than is reasonably necessary in the circumstances.

**Slide 7:**

Department Specific Acts and Policies, for example:

CSIS Act Section 18.1 (2) prevents the disclosure of any information relating to the identity of a human source.

Witness Protection Program Act: prevents the disclosure of information concerning protecting persons and methods of protection. s. 11 of WPPA (<https://laws-lois.justice.gc.ca/eng/acts/w-11.2/FullText.html>)

Income Tax Act and Excise Tax Act: While the Income Tax Act and Excise Tax Act do not contain a specific provision which would prevent the CRA from disclosing information because of national security confidentiality, all taxpayer information is protected, unless a specific exemption authorizing its disclosure is legislated; as any disclosure is discretionary, the CRA could refuse to disclose for reasons of national security

**Slide 8:**

Disclosure of Information:

Turning to the third gear, it highlights the Acts that provide for disclosure of information to the public, albeit with exceptions to ensure the safeguarding of sensitive information.

Access to Information Act -

A declassification policy was first issued in Canada through a Cabinet directive in the late 1960s, but was supplanted by the 1985 Access to Information Act. The Act remains the primary mechanism to accessing historical records, but does not require proactive disclosure. The purpose of the Act was to enhance the accountability and transparency of federal institutions to promote an open and democratic society and to enable public debate.

The ATIA provides for the right of the public to have access to information. Any exceptions associated with ATIA should be limited and specific.

**Library and Archives Act –**

This act sets out the requirements and actions of the Librarian and Archivist in maintaining records of historical and archival value. It asserts that the records must be handled according to their security classification and that no records that may be of historical and archival value shall be destroyed without the consultation with the Librarian and Archivist.

While many historical records are accessible to researchers once archived, those that remain classified will not be made accessible and will only become accessible via ATIA.

The Canada Evidence Act outlines that the accused has the right to a fair trial and the court must weigh a potential disclosure by determining whether the public interest in disclosure outweighs the importance of a specified public interest in non-disclosure.

Section 38 of the CEA prohibits an individual from disclosing sensitive or potentially injurious information during a proceeding. In such circumstances, the individual must notify the Attorney General of Canada.

**Slide 9:**

**National Security and Intelligence Committee of Parliamentarians Act -**

NSICOP in their review of national security or intelligence activities drafts reports with their review findings. Before the release of the report, if the Prime Minister believes there is information which would be injurious to national security confidentialities if released, the Prime Minister may direct the Committee to submit a revised version of the annual or special report that does not contain that information.

**National Security and Intelligence Review Agency Act -**

Similarly, NSIRA in the course of their reviews of national security and intelligence matters will complete a report on their review findings. Before the reports are released, departments review them to ensure that classified information is not publicly released. If classified information remains in the report, it will be redacted before it is released publicly.

While the reviews do not declassify and downgrade information, they do allow for information on national security and intelligence activities to be in the public domain, which increases transparency and adds to the public discourse on these issues.

**Slide 10:**

CSE publications: Annual report; Cyber Threats to Canada's Democratic Process (2017); the 2019 Update National Cyber Threat Assessment

CSIS publications: Annual report; and Issue specific ones: Foreign Interference Threats to Canada's Democratic Process (2021); Travel Security Guide, etc.

Communication Releases

Cyber Centre also routinely produces and publicly disseminates Alerts and Advisories.

**Slide 11:**

The current patchwork of legislation and policies have created some issues in current declassification and disclosure practices.

- 1) There is a general tendency for over classification of records, especially when a piece of information is taken from a highly classified document and used in another report regardless of whether the information used represents a reasonable expectation to cause injury.
- 2) The ATIA is inconsistently applied by people and organization and over time leaving individuals requesting disclosures receiving different packages of disclosed information based on the subjective interpretation of the employee reviewing the records, who is not always a subject matter expert.
- 3) The current system does not provide for proactive declassification and disclosure of information to the public. Therefore, information remains classified indefinitely until records are requested through ATIP. The system remains purely responsive and individualistic. As such, documents requested through ATIP, need to be reviewed by all implicated departments/agencies each time there is a new request.
- 4) There is no resource capacity within the Government of Canada to begin to proactively declassify and disclose information publicly, especially in light of the current backlog within the ATIP system and its legislative timeline requirements.



5) Finally, and most importantly, it is the originator who controls the classification level of the information and ultimately decides whether to declassify.

While likely unintended impacts, these issues are a reflection of the legal and policy frameworks and resources decision put in place to implement them.

The storage space and requirements associated to maintain classified documents (especially TOP SECRET documents) is very expensive and is limited. The current requirement to maintain records at the original classification level and the lack of policy direction and capacity to proactively declassify records has significantly impacted storage space requirements and is increasing the costs to the Federal Government for this purpose.

It may harm international relationships as the process for considering declassification can be time consuming and may result in 'the inability to declassify the information.

These realities are impediments to the Government of Canada successfully delivering on its commitment to transparency as part of its priority under the National Security Transparency Commitment. In so doing, it may also reduce the public's trust and confidence in the NSI community and they are unable to highlight past successes.

**Slide 12:**

Public Safety (PS), in collaboration with Treasury Board Secretariat (TBS), Library and Archives Canada (LAC) and other members of the national security and intelligence (NSI) community, has developed a draft NSI Declassification Framework.

The Framework provides guidance on a consistent and coordinated approach to declassification practices across the NSI community.

PS launched a pilot project in October 2021 to test the Framework, gather information, and assess future declassification requirements. The pilot focuses on select records (1942-1960) of the Joint Intelligence Committee (JIC) with an estimated 2.5 feet of JIC minutes and 7.5 feet of associated records. The pilot is expected to end early summer 2022.

PS also chairs an interdepartmental working group on declassification of information, with representatives from core members of the NSI community and other implicated departments, including TBS and LAC.



TBS is conducting a review of the ATI Act to inform potential reform needed to improve ATI system and address backlog. They are anticipating moving forward with an MC in relation to the ATIA in fall 2022 and submitting a report on the review to Parliament in the Fall as well.

**Slide 13:**

**Executive Order 13526 Classified National Security Information**

On December 29, 2009, the United States President Barack Obama signed an executive order (No. 13526) that prescribes a uniform system for classifying, safeguarding and declassifying national security information, including information in relation to defense against transnational terrorism.

The aim of this executive order is to balance the need to protect information critical to US national security with the need to demonstrate open transparent Government practices in classification standards and routine, secure, and effective declassification practices.

With regards to declassification, this executive order identifies that at the time of the original classification, the department of agency will establish a specific date or event when it will be declassified based on the national security sensitivity of the information. Upon reaching this date, the information will be automatically declassified.

It does stipulate that no information can be classified indefinitely, although it does allow for an original classification time period of 25 years, with the potential to extend it for an additional 25 years.

**Executive Order on Declassification Review of Certain Documents Concerning the Terrorist Attacks of September 11, 2001**

On September 3, 2021, US President Joe Biden signed an executive order to review documents associated with the terrorist attacks of September 11 for declassification. This order states that it is critical to ensure that the US Government maximizes transparency and relies on classification only narrowly tailored and when necessary. Therefore, the information collected and generated in the US Government's investigation of the 9/11 terrorist attacks should now be disclosed, except when there is the strongest reasons otherwise.

In adhering to this executive order, the US Government is to follow the December 29, 2009 executive order relating to declassification.

Further to this most recent Executive Order, the US have made recent requests to various Government of Canada departments and agencies to declassify information provided to the US relating to 9/11. The requests should be sent from the recipient US department to the originating Canadian department requesting permission to declassify and disclose the information. It is the Deputy Head's decision of the originator department to determine whether there remains an injury to the national security or defence thus whether the information can be declassified.

The US Executive Order does include exemptions when the information cannot be declassified (on the following slide).

**Slide 14:**

There are two noteworthy exceptions for the automatic declassification of information at 25 years under this order:

- (6) reveal information, including foreign government information, that would cause serious harm to relations between the United States and a foreign government, or to ongoing diplomatic activities of the United States;
- (9) violate a statute, treaty, or international agreement that does not permit the automatic or unilateral declassification of information at 25 years.

**Slide 16:**

This table, developed by Public Safety, demonstrates the governance models for the 5 Eyes Declassification Frameworks.