Protecting Democracy

Toolkit to resist DISINFORMATION and FOREIGN INTERFERENCE for PUBLIC SERVANTS

Disinformation

False information that is deliberately intended to mislead.

Foreign Interference

Deliberate and covert activities by foreign groups, state actors, or individuals to advance their interests, often to the detriment of Canada's national interests.

Our best defence against disinformation and foreign interference is to build resilience through awareness and understanding.

In Canada and around the world, democracy and democratic institutions (e.g. Parliament, provincial legislatures, the electoral process) have long faced threats from people or groups whose goal is to weaken them and weaken citizens' trust in government.

This includes disinformation - the deliberate spread of inaccurate information - and foreign interference, which have a negative effect on the well-being of people living in Canada and on Canada's unity.

As a public servant, and depending on the focus of your work, you could be become a target of disinformation or foreign interference. Individuals with input into or influence over the public policy decision-making process are attractive targets.

You may also have access to privileged information and it is your responsibility to ensure that the information is kept safe.

You can fight disinformation and help maintain the integrity of Canada's democratic institutions by being aware of these threats and by taking steps to address them.

For more information and resources, visit canada.ca/protecting-democratic-institutions and publicsafety.gc.ca.

DINSINFORMATION

Tips on how to spot disinformation

Promote a culture of accuracy. Demonstrate that you value fact-based information and encourage others to do the same.	**Pause before sharing.** Take a moment to consider the accuracy of content before drawing conclusions or sharing.
Be transparent. Acknowledge that you may not have all the information or are still waiting for confirmation.	**Share and promote accurate information, evidence, and context.** Make valid information easy to find and easy to understand.

Build resilience to disinformation by:

- ☐ understanding the public environment, and
- ☐ collaborating with others in your organization to ensure that accurate and consistent information is available.

Disinformation can be hard to spot, but there are some common signs to watch for

Look for content that:

Provokes an emotional response, particularly with negative of frightening claims	**Uses small pieces of valid information that are exaggerated or distorted**	**Manipulates photos or images by altering them or placing them out of context**	**Makes a bold or extreme statement on a controversial issue**
Contains “clickbait”: sensational and purposefully misleading headlines, images, and videos meant to entice viewers to click on specific links	**Has been shared widely on platforms with a track record of spreading disinformation**	**Makes claims that simply seem too good to be true**	

Stop the spread of disinformation

Be aware.

Disinformation is out there. You could be a target so always be on the lookout. Equip yourself with the tools to know how to identify and combat disinformation.

Be prepared.

Organizations can build resilience by planning ahead and considering the priority areas that are more vulnerable to disinformation. Recognize or anticipate possible misleading narratives that may affect your work. Know where your organization may be vulnerable.

- Start by determining your organization's priorities that could be vulnerable to disinformation.
- Understand the public environment. Consult multiple sources of information to understand what is being said about your organization, as well as where, how, and when it is being said. This can give you a clearer picture of the nature and scope of an issue or subject. Conduct a public environment analysis (PEA) to help you gather information and research data from numerous sources.
- Work within your organization to develop messages that can help fight disinformation before it happens.

Communicate.

- Provide accurate information to counter disinformation. Offer reliable facts in a clear, timely manner.
- Fill the information space with accurate and helpful information, through frequent communication using different methods which may include press conferences and media technical briefings, backgrounders to provide additional and contextual information, government website updates, and posts on official social media accounts.
- Ensure your messaging is clear and concise. Use plain language.

Correct it.

To debunk disinformation means to expose false information, directly, with the aim of clarifying the facts.

- Fact-check claims by using credible sources and provide accurate counterevidence to the false narrative.
- Back up your corrections with credible sources and evidence. Provide links, references, or citations to reputable sources that support your statements.

FOREIGN INTERFERENCE

Foreign interference can erode trust and threaten the integrity of our democratic institutions, political system, fundamental rights and freedoms, and ultimately, our sovereignty. No matter the department, classification, or level, public servants and others with input into, or influence over, the public policy decision-making process can be targeted by foreign actors.

Foreign state actors use a variety of techniques to target all aspects of civil society, such as diverse communities, electoral processes, post-secondary campuses, and traditional and social media. Common techniques or activities used by foreign state actors can include elicitation, cultivation, coercion, illicit financing, cyber-incidents, intimidation, and disinformation.

Unlike legitimate international cooperation and diplomacy which is transparent and done in good faith, foreign interference is covert and malign. Some other concerning signals to watch for include:

- ☐ a lack of transparency around communications, relationships, behaviour and interactions
- ☐ suggestions or implications that interaction will result in an exchange of favours or advantages (quid pro quo)
- ☐ offers of unusually generous gifts, travel or other benefits
- ☐ pressure to influence others to support particular views, opinions or positions

Protect yourself and your department from foreign interference

Be proactive: Protect yourself, your organization, your reputation, and your work by being aware of the threat and performing due diligence.

Be prepared. Develop policies, procedures and processes for dealing with instances of foreign interference. Make these public to ensure that potential threat actors are aware that you will not tolerate foreign interference activities. You may wish to consult Departmental Security Officers and the policies in place within your organization.

Educate. Provide awareness materials, training and guidance on associated policies and procedures to all employees and contractors.

Report it. Suspicious activities and any incidents of intimidation, harassment, coercion, or threats should be reported to your departmental Chief Security Officer, your local law enforcement authorities or to the Canadian Security Intelligence Service (CSIS).

For more information on ways to protect yourself from foreign interference, consult Foreign Interference and You and Protect yourself from foreign interference.

How to report foreign interference in Canada

Any individual in Canada who is concerned that they are being targeted by state or non-state actors for the purposes of foreign interference should contact local police or the **Royal Canadian Mounted Police's (RCMP) National Security Information Network** at 1-800-420-5805, or by email at RCMP.NSIN-RISN.GRC@rcmp-grc.gc.ca.

Report espionage or foreign interference to the **Canadian Security Intelligence Service (CSIS)** at 613-993-9620 or 1-800-267-7685, or online.

ISBN: 978-0-660-68170-2
CP22-207/3-2023E-PDF