Private Sector Breach Reporting and Notification Requirements:
Privacy Legislation and Additional Rules for Selected Regulated Industries

Table of Contents:

Source of Breach Reporting and Notification Requirements	Entities Subject to the Requirements	Type of Requirement	Page
Private Sector Privacy Legislation			
Personal Information Protection and Electronic Documents Act ("PIPEDA")	Federal private sector organizations	Statutory requirement, with accompanying regulations	3
Alberta *Personal Information Protection Act* ("PIPA AB")	Alberta private sector organizations	Statutory requirement, with accompanying regulations	6
Quebec *Act Respecting the Protection of Personal Information in the Private Sector*	Quebec private sector organizations	Statutory requirement, with accompanying regulations	8
Industry-Specific Requirements			
Office of the Superintendent of Financial Institutions (OSFI) - Technology and Cyber Security Incident Reporting Advisory	Federally regulated financial institutions (FRFIs)	Regulatory advisory	13
Canadian Securities Administrators (CSA) - Multilateral Staff Notice 51-347 – Disclosure of cyber security risks and incidents	Issuers, registrants and entities regulated under provincial securities regimes	Regulatory staff notice	13
Investment Industry Regulatory Organization of Canada (IIROC) – IIROC Rule 3703	Regulated member dealers	Regulatory rule	14
Bank of Canada - Guideline for Cyber and Information Technology Incident Reporting	Financial market infrastructures (FMIs)	Guideline	15
Marine Transportation Security Regulations, issued under the federal *Marine Transportation Security Act*	Canadian vessels governed by the *Marine Transportation Security Act*	Regulation	15
North American Electric Reliability Corporation (NERC) - Critical Infrastructure	NERC-regulated entities in the electricity industry in Canada, the United States, and Mexico	International regulatory authority standard	16

Source of Breach Reporting and Notification Requirements	Entities Subject to the Requirements	Type of Requirement	Page
Protection (CIP) Cyber Security Standards; CIP-008-5			
Nuclear Safety and Control Act	Entities licensed by the Canadian Nuclear Safety Commission	Statutory requirements, with accompanying regulations	17
Ontario *Child, Youth and Family Services Act, 2017*	Service Providers in the children's aid industry, as defined in s. 2 of the legislation	Statutory requirement, with accompanying regulations	21
Quebec *Regulation respecting the management and reporting of information security incidents by certain financial institutions and by credit assessment agents*, issued under the Quebec *Credit Assessment Agents Act, Insurers Act, Act respecting financial services cooperatives, Deposit Institutions and Deposit Protection Act,* and *Trust Companies and Savings Companies Act*	Financial institutions governed by the Quebec *Credit Assessment Agents Act, Insurers Act, Act respecting financial services cooperatives, Deposit Institutions and Deposit Protection Act,* and *Trust Companies and Savings Companies Act*	Regulation	24

Private Sector Privacy Legislation – Breach Reporting and Notification Requirements					
Legislation	**Reporting and Notification Threshold**	**Timing of Reporting and Notification**	**Method/Manner of Reporting and Notification**	**Content of Reporting and Notification**	**Penalties**
Personal Information Protection and Electronic Documents Act ("PIPEDA"), with accompanying regulations	• An organization shall report to the Commissioner any breach of security safeguards involving personal information under its control if it is reasonable in the circumstances to believe that the breach creates a real risk of significant harm to an individual (s.10.1 (1)) • For the purpose of this section, "significant harm" includes bodily harm, humiliation, damage to reputation or relationships, loss of employment, business or professional opportunities, financial loss, identity theft, negative effects on the credit record and damage to or loss of property. (s. 10.1(7)) • The factors that are relevant to determining whether a breach of security safeguards creates a real risk of significant harm to the individual include **(a)** the sensitivity of the personal information involved in the breach; **(b)** the probability that the personal information has been, is being or will be misused; and **(c)** any other prescribed factor. (s. 10.1(8)) • Unless otherwise prohibited by law, an organization shall notify an individual of any breach of security safeguards involving the individual's personal	• The report shall contain the prescribed information and shall be made in the prescribed form and manner as soon as feasible after the organization determines that the breach has occurred. (10.1(2)) • 2(1) A report of a breach of security safeguards referred to in subsection 10.1(2) of the Act must be in writing and must contain (a) a description of the circumstances of the breach and, if known, the cause; (b) the day on which, or the period during which, the breach occurred or, if neither is known, the approximate period;	• The notification shall be conspicuous and shall be given directly to the individual in the prescribed form and manner, except in prescribed circumstances, in which case it shall be given indirectly in the prescribed form and manner. (10.1(5)) • For the purposes of subsection 10.1(5) of the Act, direct notification must be given to the affected individual in person, by telephone, mail, email or any other form of communication that a reasonable person would consider appropriate in the circumstances. (s. 4, *Breach of Security*	• The report shall contain the prescribed information and shall be made in the prescribed form and manner as soon as feasible after the organization determines that the breach has occurred.(s. 10.1(2)) • The notification shall contain sufficient information to allow the individual to understand the significance to them of the breach and to take steps, if any are possible, to reduce the risk of harm that could result from it or to mitigate that harm. It shall also contain any other prescribed information. (s. 10.1(4)) • A notification provided by an organization, in accordance with subsection 10.1(3) of the Act, to an affected individual with respect to a breach of security safeguards must contain: (a) a description of the circumstances of the breach; (b) the day on which, or period during which, the breach occurred or, if neither is known, the approximate period; (c) a description of the personal information that is the subject of the breach to the extent that the information is known; (d) a description of the steps that the organization has taken to reduce the risk of harm that could result from the breach; (e) a description of the steps that affected individuals could take to reduce the risk of harm that could result from the breach or to mitigate that harm; and	• Every organization that knowingly contravenes subsection 8(8), section 10.1 or subsection 10.3(1) or 27.1(1) or that obstructs the Commissioner or the Commissioner's delegate in the investigation of a complaint or in conducting an audit is guilty of (a) an offence punishable on summary conviction and liable to a fine not exceeding $10,000; or (b) an indictable offence and liable to a fine

Private Sector Privacy Legislation – Breach Reporting and Notification Requirements					
Legislation	**Reporting and Notification Threshold**	**Timing of Reporting and Notification**	**Method/Manner of Reporting and Notification**	**Content of Reporting and Notification**	**Penalties**
	information under the organization's control if it is reasonable in the circumstances to believe that the breach creates a real risk of significant harm to the individual. (s. 10.1(3)) • An organization that notifies an individual of a breach of security safeguards under subsection 10.1(3) shall notify any other organization, a government institution or a part of a government institution of the breach if the notifying organization believes that the other organization or the government institution or part concerned may be able to reduce the risk of harm that could result from it or mitigate that harm, or if any of the prescribed conditions are satisfied. (s. 10.2(1)) • In addition to the circumstances set out in subsection 7(3), for the purpose of clause 4.3 of Schedule 1, and despite the note that accompanies that clause, an organization may disclose personal information without the knowledge or consent of the individual if (a) the disclosure is made to the other organization, the government institution or the part of a government institution that was notified of the breach under subsection (1); and (b) the disclosure is made solely for the purposes of reducing the risk of harm to the individual that could	(c) a description of the personal information that is the subject of the breach to the extent that the information is known; (d) the number of individuals affected by the breach or, if unknown, the approximate number; (e) a description of the steps that the organization has taken to reduce the risk of harm to affected individuals that could result from the breach or to mitigate that harm; (f) a description of the steps that the organization has taken or intends to take to notify affected individuals of the breach in accordance with subsection	*Safeguards Regulations*) • For the purposes of subsection 10.1(5) of the Act, indirect notification must be given by an organization in any of the following circumstances: (a) direct notification would be likely to cause further harm to the affected individual; (b) direct notification would be likely to cause undue hardship for the organization; or (c) the organization does not have contact information for the affected individual. (PIPEDA Breach Reg s. 5(1))	(f) contact information that the affected individual can use to obtain further information about the breach. (PIPEDA Breach Reg s. 3) • An organization shall, in accordance with any prescribed requirements, keep and maintain a record of every breach of security safeguards involving personal information under its control. (10.3(1)) • An organization shall, on request, provide the Commissioner with access to, or a copy of, a record. (s. 10.3(2)) • For the purposes of subsection 10.3(1) of the Act, an organization must maintain a record of every breach of security safeguards for 24 months after the day on which the organization determines that the breach has occurred. (PIPEDA Breach Reg. s. 6(1)) • The record referred to in subsection 10.3(1) of the Act must contain any information that enables the Commissioner to verify compliance with subsections 10.1(1) and (3) of the Act. (PIPEDA Breach Reg. s. 6(2))	not exceeding $100,000 (s. 28)

Private Sector Privacy Legislation – Breach Reporting and Notification Requirements					
Legislation	**Reporting and Notification Threshold**	**Timing of Reporting and Notification**	**Method/Manner of Reporting and Notification**	**Content of Reporting and Notification**	**Penalties**
	result from the breach or mitigating the harm. (s. 10.2(3)) • Despite clause 4.5 of Schedule 1, an organization may disclose personal information for purposes other than those for which it was collected in the circumstance set out in subsection (3). (s. 10.2(4))	10.1(3) of the Act; and (g) the name and contact information of a person who can answer, on behalf of the organization, the Commissioner's questions about the breach. (PIPEDA Breach Reg. ss. 2(1)) • An organization may submit to the Commissioner any new information referred to in subsection (1) that the organization becomes aware of after having made the report (PIPEDA Breach Reg. ss. 2(2)). • The report may be sent to the Commissioner by any secure means of communication (PIPEDA Breach Reg. ss. 2(3)).	• For the purposes of subsection 10.1(5) of the Act, indirect notification must be given by public communication or similar measure that could reasonably be expected to reach the affected individuals. PIPEDA Breach Reg s 5(2))		

Private Sector Privacy Legislation – Breach Reporting and Notification Requirements					
Legislation	**Reporting and Notification Threshold**	**Timing of Reporting and Notification**	**Method/Manner of Reporting and Notification**	**Content of Reporting and Notification**	**Penalties**
		• The notification shall be given as soon as feasible after the organization determines that the breach has occurred. (s. 10.1(6)) • The notification shall be given as soon as feasible after the organization determines that the breach has occurred. (s. 10.2(2))			
Alberta *Personal Information Protection Act* ("PIPA AB"), and accompanying regulations	• An organization having personal information under its control must, without unreasonable delay, provide notice to the Commissioner of any incident involving the loss of or unauthorized access to or disclosure of the personal information where a reasonable person would consider that there exists a real risk of significant harm to an individual as a result of the loss or unauthorized access or disclosure. (ss. 34.1(1)) • A notice to the Commissioner under subsection (1) must include the	• An organization having personal information under its control must, without unreasonable delay, provide notice to the Commissioner of any incident involving the loss of or unauthorized access to or disclosure of the personal information (s. 34.1(1))	• A notice provided by an organization to the Commissioner under section 34.1(1) of the Act must be in writing and include certain prescribed information (s. 19, *PIPA Regulation*)	• **Report requirements:** A notice provided by an organization to the Commissioner under section 34.1(1) of the Act must be in writing and include the following information: (a) a description of the circumstances of the loss or unauthorized access or disclosure; (b) the date on which or time period during which the loss or unauthorized access or disclosure occurred; (c) a description of the personal information involved in the loss or unauthorized access or disclosure;	**Penalties:** (1) Subject to subsections (3) and (4), a person commits an offence if the person (e.1) fails to provide notice to the Commissioner under section 34.1; (s. 59(1)(e.1)) (2) A person who commits an offence under subsection (1)

Private Sector Privacy Legislation – Breach Reporting and Notification Requirements					
Legislation	**Reporting and Notification Threshold**	**Timing of Reporting and Notification**	**Method/Manner of Reporting and Notification**	**Content of Reporting and Notification**	**Penalties**
	information prescribed by the regulations. (ss. 34.1(2)) • Where an organization suffers a loss of or unauthorized access to or disclosure of personal information that the organization is required to provide notice of under section 34.1, the Commissioner may require the organization to notify individuals to whom there is a real risk of significant harm as a result of the loss or unauthorized access or disclosure (a) in a form and manner prescribed by the regulations, and (b) within a time period determined by the Commissioner…. (s. 37.1)	• Where an organization suffers a loss of or unauthorized access to or disclosure of personal information that the organization is required to provide notice of under section 34.1, the Commissioner may require the organization to notify individuals to whom there is a real risk of significant harm as a result of the loss or unauthorized access or disclosure (b) within a time period determined by the Commissioner. (s. 37.1(1))		(d) an assessment of the risk of harm to individuals as a result of the loss or unauthorized access or disclosure; (e) an estimate of the number of individuals to whom there is a real risk of significant harm as a result of the loss or unauthorized access or disclosure; (f) a description of any steps the organization has taken to reduce the risk of harm to individuals; (g) a description of any steps the organization has taken to notify individuals of the loss or unauthorized access or disclosure; (h) the name of and contact information for a person who can answer, on behalf of the organization, the Commissioner's questions about the loss or unauthorized access or disclosure. (s. 19, *PIPA Regulation*) • Where an organization is required under section 37.1 of the Act to notify an individual to whom there is a real risk of significant harm as a result of a loss of or unauthorized access to or disclosure of personal information, the notification must **(a)** be given directly to the individual, and **(b)** include: (i) a description of the circumstances of the loss or unauthorized access or disclosure, (ii) the date on which or time period during which the loss or unauthorized access or disclosure occurred,	is liable, (a) in the case of an individual, to a fine of not more than $10 000, and (b)in the case of a person other than an individual, to a fine of not more than $100 000. (s. 59(2)) (3) No person is liable to prosecution for an offence against this or any other Act by reason only of complying with a requirement of the Commissioner under this Act. (s. 59(3)) (4) Neither an organization nor an individual is guilty of an offence under this Act if it is established to the satisfaction of the court that the organization or individual, as the

Private Sector Privacy Legislation – Breach Reporting and Notification Requirements					
Legislation	**Reporting and Notification Threshold**	**Timing of Reporting and Notification**	**Method/Manner of Reporting and Notification**	**Content of Reporting and Notification**	**Penalties**
				(iii) a description of the personal information involved in the loss or unauthorized access or disclosure, (iv) a description of any steps the organization has taken to reduce the risk of harm, and (v) contact information for a person who can answer, on behalf of the organization, questions about the loss or unauthorized access or disclosure. (s. 19.1) Notwithstanding subsection (1)(a), where an organization is required to notify an individual under section 37.1 of the Act, the notification may be given to the individual indirectly if the Commissioner determines that direct notification would be unreasonable in the circumstances. (s. 19.1(2))	case may be, acted reasonably in the circumstances that gave rise to the offence. (s. 59(4))
Quebec *Act Respecting the Protection of Personal Information in the Private Sector*, with accompanying regulations NOTE: the notification obligations in this section came into force in **September**	• Any person carrying on an enterprise who has cause to believe that a confidentiality incident involving personal information the person holds has occurred must take reasonable measures to reduce the risk of injury and to prevent new incidents of the same nature. (s 3.5) • "confidentiality incident" means (1) access not authorized by law to personal information; (2) use not authorized by law of personal information;	• If the incident presents a risk of serious injury, the person carrying on an enterprise must promptly notify the Commission d'accès à l'information and any affected individuals (unless doing so would hamper a legal investigation into a crime or statutory offence). (s 3.5)	• Notices shall be sent to the persons concerned by the confidentiality incident. (s. 6, *Confidentiality Incident Regulations*) • Despite this, the notices can be given by way of a public notice in any of the following circumstances:	• Notices to the CAI that a confidentiality incident presents a risk of services injury, given under s. 3.5 of the Act, must be in writing and must contain: (1) The name of the body affected by the confidentiality incident and any Québec business number assigned to such body under the Act respecting the legal publicity of enterprises; (2) the name and contact information of the person to be contacted in that body with regard to the incident; (3) a description of the personal information covered by the incident or, if that information is not known, the reasons why it is impossible to provide such a description; (4) a brief description of the circumstances of the incident and what caused it, if known;	A monetary administrative penalty may be imposed by a person designated by the Commission, but who is not a member of any of its divisions, on anyone who.. (3) does not report, where required to do so, a confidentiality incident to the Commission or to the persons

Private Sector Privacy Legislation – Breach Reporting and Notification Requirements					
Legislation	**Reporting and Notification Threshold**	**Timing of Reporting and Notification**	**Method/Manner of Reporting and Notification**	**Content of Reporting and Notification**	**Penalties**
2022 (Bill 62, s. 175).	(3) communication not authorized by law of personal information; or (4) loss of personal information or any other breach in the protection of such information. (s 3.6) • If the incident presents a risk of serious injury, the person carrying on an enterprise must promptly notify the Commission d'accès à l'information. He must also notify any person whose personal information is concerned by the incident, failing which the Commission may order him to do so. He may also notify any person or body that could reduce the risk, by communicating to the person or body only the personal information necessary for that purpose without the consent of the person concerned. In the latter case, the person in charge of the protection of personal information must record the communication of the information. (s. 3.5) • A person whose personal information is concerned by the incident need not be notified so long as doing so could hamper an investigation conducted by a person or body responsible by law for the	• A person or body carrying out a mandate or performing a contract of enterprise or for services referred to in the first paragraph must notify the person in charge of the protection of personal information without delay of any violation or attempted violation by any person of any obligation concerning the confidentiality of the information communicated, and must also allow the person in charge of personal information to conduct any verification relating to confidentiality requirements. (s 18.3)	(1) when the fact of sending such notice is likely to cause increased injury to the person concerned; (2) when the fact of sending such notice is likely to cause undue hardship for the body; (3) when the body does not have the contact information for the person concerned. (s. 6, *Confidentiality Incident Regulations*) • The notices referred to in section 5 may also be given by way of a public notice if there is a need to act rapidly to reduce the risk of a serious injury or to mitigate any such injury. In such cases, the body must still send a	(5) the date or time period when the incident occurred or, if that is not known, the approximate time period; (6) the date or time period when the body became aware of the incident; (7) the number of persons concerned by the incident and the number of those who reside in Québec or, if that is not known, the approximate numbers; (8) a description of the elements that led the body to conclude that there is a risk of serious injury to the persons concerned, such as the sensitivity of the personal information concerned, any possible ill-intentioned uses of such information, the anticipated consequences of its use and the likelihood that such information will be used for injurious purposes; (9) the measures the body has taken or intends to take to notify the persons whose personal information is concerned by the incident, pursuant to the second paragraph of section 3.5 of the Act respecting the protection of personal information in the private sector, and the date on which such persons were notified, or the expected time limit for the notification; (10) the measures the body has taken or intends to take after the incident occurred, including those aimed at reducing the risk of injury or mitigating any such injury and those aimed at preventing new incidents of the same nature, and the date or time period on which the measures were taken or the expected time limit for taking the measures; and	concerned. (ss 90.1(3)) • The maximum amount of the monetary administrative penalty is $50,000 in the case of a natural person and, in all other cases, $10,000,000 or, if greater, the amount corresponding to 2% of worldwide turnover for the preceding fiscal year. (s 90.12) • Anyone who (2) fails to report, where required to do so, a confidentiality incident to the Commission or to the persons concerned.. commits an offence and is

Private Sector Privacy Legislation – Breach Reporting and Notification Requirements					
Legislation	**Reporting and Notification Threshold**	**Timing of Reporting and Notification**	**Method/Manner of Reporting and Notification**	**Content of Reporting and Notification**	**Penalties**
	prevention, detection or repression of crime or statutory offences. (s. 3.5) • In assessing the risk of injury to a person whose personal information is concerned by a confidentiality incident, a person carrying on an enterprise must consider, in particular, the sensitivity of the information concerned, the anticipated consequences of its use and the likelihood that such information will be used for injurious purposes. The person must also consult the person in charge of the protection of personal information within the enterprise. (s. 3.7) • A person or body carrying out a mandate or performing a contract of enterprise or for services referred to in the first paragraph must notify the person in charge of the protection of personal information without delay of any violation or attempted violation by any person of any obligation concerning the confidentiality of the information communicated, and must also allow the person in charge of personal information to conduct any verification relating to confidentiality requirements. (s. 18.3)		notice to the person concerned with proper diligence, unless one of the circumstances listed in the second paragraph applies. (s. 6, *Confidentiality Incident Regulations*) • Pursuant to this section, public notices may be made by any method that could be reasonably expected to reach the person concerned. (s. 6, *Confidentiality Incident Regulations*)	(11) if applicable, an indication that a person or body outside Québec that exercises similar functions to those of the Commission d'accès à l'information with respect to overseeing the protection of personal information has been notified of the incident. (s. 3) • Notices to persons whose personal information is concerned by a confidentiality incident presenting a risk of serious injury, given under the section 3.5 of the Act, must contain: (1) a description of the personal information covered by the incident or, if that information is not known, the reasons why it is impossible to provide such a description; (2) a brief description of the circumstances of the incident; (3) the date or the time period when the incident occurred or, if that is not known, the approximate time period. (4) a brief description of the measures the body has taken or intends to take after the incident occurred in order to reduce the risks of injury; (5) the measures that the body suggests the person concerned take in order to reduce the risk of injury or mitigate any such injury; and (6) the contact information where the person concerned may obtain more information about the incident. (s. 5, *Confidentiality Incident Regulations*) • A person carrying on an enterprise must keep a register of confidentiality incidents. A government regulation may	liable to a fine of $5,000 to $100,000 in the case of a natural person and, in all other cases, of $15,000 to $25,000,000 or, if greater, the amount corresponding to 4% of worldwide turnover for the preceding fiscal year. (s 91) • In the case of a subsequent offence, the fines under this division are doubled (s 92.1) • Where the unlawful infringement of a right conferred by this Act or by articles 35 to 40 of the Civil Code causes an

Private Sector Privacy Legislation – Breach Reporting and Notification Requirements					
Legislation	**Reporting and Notification Threshold**	**Timing of Reporting and Notification**	**Method/Manner of Reporting and Notification**	**Content of Reporting and Notification**	**Penalties**
				determine the content of the register. A copy of the register must be sent to the Commission at its request. (s 3.8) • The register provided for in s. 3.8 of the Act must contain: (1) a description of the personal information covered by the incident or, if that information is not known, the reasons why it is impossible to provide such a description; (2) a brief description of the circumstances of the incident; (3) the date or time period when the incident occurred or, if that is not known, the approximate time period; (4) the date or time period when the body became aware of the incident; (5) the number of persons concerned by the incident or, if that is not known, the approximate number; (6) a description of the elements that led the body to conclude whether or not there is a risk of serious injury to the persons concerned, such as the sensitivity of the personal information concerned, any possible ill-intentioned uses of such information, the anticipated consequences of its use and the likelihood that such information will be used for injurious purposes; (7) if the incident presents a risk of serious injury, the transmission dates of the notices to the CAI and the persons concerned, pursuant to the second paragraph of section 3.5 of	injury and the infringement is intentional or results from a gross fault, the court shall award punitive damages of not less than $1,000. (s 93.1)

Private Sector Privacy Legislation – Breach Reporting and Notification Requirements					
Legislation	**Reporting and Notification Threshold**	**Timing of Reporting and Notification**	**Method/Manner of Reporting and Notification**	**Content of Reporting and Notification**	**Penalties**
				the Act, as well as an indication of whether the body issued public notices and, if applicable, its reasons for doing so; and (8) a brief description of the measures the body has taken after the incident occurred in order to reduce the risks of injury. (s. 7, *Confidentiality Incident Regulations*) • The information in the registers must be kept up to date and kept for at least 5 years after the date or time period when the body became aware of the incident. (s. 8, *Confidentiality Incident Regulations*)	

Industry-Specific Requirements					
Requirement	**Reporting Threshold**	**Timing of Reporting**	**Method/Manner of Reporting**	**Content of Reporting**	**Penalties**
Office of the Superintendent of Financial Institutions (OSFI) - Technology and Cyber Security Incident Reporting Advisory	• Federally Regulated Financial Institutions (FRFIs) must report a technology or cyber security incident to OSFI's Technology Risk Division as well as their Lead Supervisor at OSFI. • A technology or cyber security incident is defined as an incident that has an impact, or the potential to have an impact, on the operations of a FRFI, including its confidentiality, integrity or the availability of its systems and information.	• FRFIs must report a technology or cyber security incident to OSFI's Technology Risk Division as well as their Lead Supervisor at OSFI within 24 hours, or sooner if possible.	When reporting a technology or cyber security incident to OSFI, a FRFI must notify OSFI's Technology Risk Division (at TRD@osfi-bsif.gc.ca) as well as their Lead Supervisor and must do so in writing as set out in the Incident Reporting and Resolution Form (see Appendix II).	• Where specific details are unavailable at the time of the initial report, the FRFI must indicate 'information not yet available.' In such cases, the FRFI must provide best estimates and all other details available at the time including their expectations of when additional information will be available. • OSFI expects FRFIs to provide regular updates (e.g., daily) as new information becomes available, and until all details about the incident have been provided. • Until the incident is contained/resolved, OSFI expects FRFIs to provide situation updates, including any short term and long-term remediation actions and plans. • Following incident containment, recovery and closure, the FRFI should report to OSFI on its post-incident review and lessons learned.	• Failure to report incidents as outlined above may result in increased supervisory oversight including but not limited to enhanced monitoring activities, watch-listing or staging of the FRFI.
Canadian Securities Administrators (CSA) - Multilateral Staff Notice 51-347 – Disclosure of cyber security risks and incidents	• In considering whether and when to disclose a cyber security incident, the issuer must determine whether it is a material fact or material change that requires disclosure in accordance with securities legislation. • The issuer should refer to the guidance in National Policy 51-201 *Disclosure Standards* and may in addition refer to the provisions of Part 1(f) of Form 51-			Where an issuer has determined a cyber security incident should be disclosed, it might be appropriate to consider and provide visibility as to the anticipated impact and costs of the incident.	

Industry-Specific Requirements					
Requirement	**Reporting Threshold**	**Timing of Reporting**	**Method/Manner of Reporting**	**Content of Reporting**	**Penalties**
	102F1 *Management's Discussion & Analysis* and Part 1(e) of Form 51-102F2 A*nnual Information Form* of National Instrument 51-102 *Continuous Disclosure Obligations*.				
Investment Industry Regulatory Organization of Canada (IIROC) – IIROC Rule 3703	(2) A Dealer Member must report to IIROC any of the following matters, within the time period and using the method prescribed by IIROC: (vii) any cybersecurity incident, in writing, (1) For purposes of this section 3703, a "cybersecurity incident" includes any act to gain unauthorized access to, disrupt or misuse a *Dealer Member*'s information system, or information stored on such information system, that has resulted in, or has a reasonable likelihood of resulting in: • substantial harm to any *person*, • a material impact on any part of the normal operations of the *Dealer Member*, • invoking the *Dealer Member's* business continuity plan or disaster recovery plan, or • the *Dealer Member* being required under any *applicable laws* to provide notice to any government	(a) within three calendar days from discovering a cybersecurity incident,	A Dealer Member must report to IIROC a cybersecurity incident in writing (2)(vii)	(a) within three calendar days from discovering a cybersecurity incident, and must include the following information: (I) a description of the cybersecurity incident, (II) the date on which or time period during which the cybersecurity incident occurred and the date it was discovered by the Dealer Member, (III) a preliminary assessment of the cybersecurity incident, including the risk of harm to any person and/or impact on the operations of the Dealer Member, (IV) a description of immediate incident response steps the Dealer Member has taken to mitigate the risk of harm to persons and impact on its operations, and (V) the name of and contact information for an individual who can answer, on behalf of the Dealer Member, any of IIROC's follow-up questions about the cybersecurity incident, b) within 30 calendar days, unless otherwise agreed by IIROC, from discovering a cybersecurity incident, and must include the following information: (I) a description of the cause of the cybersecurity incident, (II) an assessment of the scope of the cybersecurity incident, including the number of persons harmed and the impact on the operations of the Dealer Member, (III) details of the steps the Dealer Member took to mitigate the risk of harm to persons and impact on its operations,	

Industry-Specific Requirements					
Requirement	**Reporting Threshold**	**Timing of Reporting**	**Method/Manner of Reporting**	**Content of Reporting**	**Penalties**
	body, *securities regulatory authority* or other self-regulatory organization.			(IV) details of the steps the Dealer Member took to remediate any harm to any persons, and (V) actions the Dealer Member has or will take to improve its cybersecurity incident preparedness.	
Bank of Canada - Guideline for Cyber and Information Technology Incident Reporting	The Bank expects Financial market infrastructures (FMIs) to report all cyber and IT incidents (hereafter referred to as incidents) that are material to the FMI (i.e., the clearing and settlement system and/or its operator). Materiality is defined in relation to its impact on the FMI, whether direct or indirect.	Upon identification of a material incident, FMIs are expected to immediately notify the director responsible for oversight of the FMI	Details of the incident are to be sent in writing, copying the senior director of the Bank's oversight division and any other contacts that the Bank has specified.	The FMI should provide updates if there are changes in the status of the incident, at a minimum at resumption of service and once the incident has been fully rectified. FMIs are expected to use the Bank's operational incident reporting template to communicate the details of the incident, updating the template as required at specific points during the lifecycle of the cyber incident.	
Marine Transportation Security Regulations, issued under the federal *Marine Transportation Security Act*	212 A vessel security officer shall (j) report security breaches to the Minister and, if applicable, the port administration, as soon as possible after they occur; 306 A marine facility security officer shall (k) report security breaches to the Minister and, if applicable, the port administration, as soon as possible after they occur; security breach means a violation of these Regulations, of a security measure formulated under subsection 7(1) of the Act, of a security rule formulated under subsection 10(2) or (3) of the Act, or of a security procedure set out in an approved				

Industry-Specific Requirements					
Requirement	**Reporting Threshold**	**Timing of Reporting**	**Method/Manner of Reporting**	**Content of Reporting**	**Penalties**
	security plan or approved under subsection 360(1), that does not result in a security incident.				
North American Electric Reliability Corporation (NERC) - Critical Infrastructure Protection (CIP) Cyber Security Standards; CIP-008-5	No later than 90 calendar days after completion of a Cyber Security Incident response plan(s) test or actual Reportable Cyber Security Incident response: 3.1.1. Document any lessons learned or document the absence of any lessons learned; 3.1.2. Update the Cyber Security Incident response plan based on any documented lessons learned associated with the plan; and 3.1.3. Notify each person or group with a defined role in the Cyber Security Incident response plan of the updates to the Cyber Security Incident response plan based on any documented lessons learned. For Part 1.2, a Reportable Cyber Security Incident is a Cyber Security Incident that has compromised or disrupted one or more reliability tasks of a functional entity.	The reporting obligations for Reportable Cyber Security Incidents require at least a preliminary notice to the ES-ISAC within one hour after determining that a Cyber Security Incident is reportable (not within one hour of the Cyber Security Incident, an important distinction). This standard does not require a complete report within an hour of determining that a Cyber Security Incident is reportable, but at least preliminary notice, which may be a phone call, an email, or sending a	Initial notification to the ES-ISAC, which may be only a preliminary notice, shall not exceed one hour from the determination of a Reportable Cyber Security Incident. No later than 90 calendar days after completion of a Cyber Security Incident response plan(s) test or actual Reportable Cyber Security Incident response:		

Industry-Specific Requirements					
Requirement	**Reporting Threshold**	**Timing of Reporting**	**Method/Manner of Reporting**	**Content of Reporting**	**Penalties**
		Web-based notice. The standard does not require a specific timeframe for completing the full report.			
Federal *Nuclear Safety and Control Act* and General Nuclear Safety and Control Regulations	29. (1) Every licensee who becomes aware of any of the following situations shall immediately make a preliminary report to the Commission of the location and circumstances of the situation and of any action that the licensee has taken or proposes to take with respect to it: (e) an attempted or actual breach of security or an attempted or actual act of sabotage at the site of the licensed activity; Specific reporting provisions The licensee shall report on: a) any attempted or actual breach against electronic systems and/or subsystems critical for safety, security and emergency preparedness of the NPP b) any security incident in the form of: i. a misuse of security-related equipment that may result in a security and/or safety vulnerability	Immediate reporting is required only where a hazard to the health, safety and security of persons and the environment or to the security of the nuclear facility exists. preliminary event reports due immediately for a significant breach or within 5 business days of determination of reportability for a non-significant breach detailed event report due in 60 days (if required)	An event report that must be submitted immediately may be made orally or filed in writing; an event report made orally shall be followed by a written event report within five business days of the oral event report submission If any required information is missing from an event report, the licensee shall file all of the required missing detailed information within 60 days of filing an original event report for significant	All reports filed by the licensee according to this regulatory document shall contain the name and address of the sender of the report and the date of completion of the report. The licensee shall mark all reports made or filed under this regulatory document with an appropriate protection and classification and shall file reports under the appropriate security precautions A preliminary event report or an immediate notification shall contain the following information as far as practicable and applicable: 1. date, time and circumstances of the discovery of the situation or event, or notification 2. date and time of the onset (removal, reinstatement) and the duration of the situation or event 3. unique identification reference for the report for record tracking purposes 4. a reporting provision that best describes the situation(s) or event(s) 5. identification of the affected NPP and associated reactor units 6. identification of the affected structures, systems and components, including:	*Nuclear Safety and Control Act* 48 Every person commits an offence who ..(k) fails to comply with this Act or any regulation made pursuant to this Act. 51(3) Every person who commits an offence other than an offence in respect of which subsection (1) or (2) applies a. is guilty of an indictable offence and liable to a fine not exceeding $1,000,000 or to imprisonment for a term not exceeding

Industry-Specific Requirements					
Requirement	**Reporting Threshold**	**Timing of Reporting**	**Method/Manner of Reporting**	**Content of Reporting**	**Penalties**
	ii. the discharge of firearms or the application of use of force options iii. a credible threat made against the NPP The licensee shall use a safety significance classification system as documented in its management system to determine the safety significance of a situation or event		situations or events; otherwise, the licensee shall notify the CNSC that an extension is necessary and provide a date when the missing detailed information will be submitted	a. the design flow diagram reference number(s) b. material type and code classification c. design and hydrostatic test pressure of the system d. magnitude, size or quantification of the degradation or fault (e.g., approximate size, length, depth or leak rates, deviation from set point) 7. description of the occurrence and consequences of the situation or event, including: a. the condition of the site where the situation or event has occurred and the operating conditions, immediately prior, during and after of any power reactor unit involved in the situation or event b. the safety and control functions affected c. causes, circumstances, consequences and effects of the degradation d. a description of any secondary events that occur as a result of the primary reportable event, that may be of regulatory interest e. code, standard or methodology used to assess the significance of the degradation f. a summary of any impairment of a special safety system or safety-related system g. reasons for removal of certified persons	five years or to both; or b. is guilty of an offence punishable on summary conviction and liable to a fine not exceeding $500,000 or to imprisonment for a term not exceeding eighteen months or to both.

Industry-Specific Requirements					
Requirement	**Reporting Threshold**	**Timing of Reporting**	**Method/Manner of Reporting**	**Content of Reporting**	**Penalties**
				8. identification of persons affected by the situation or event a. including any exposure of a person to radiation b. removal or reinstatement of a certified person from the duties of the position for which the person is certified by the CNSC c. revocation of authorization by the licensee 9. a description of any actions and/or remedial actions the licensee has taken or proposes to take with respect to the situation or event 10. a description of the research or analysis that led to awareness of the problem or potential problem 11. the name of the nuclear or hazardous substance released, the estimated or measured quantity of the unauthorized released, the estimated or measured rate of release, and the manner of release, the offsite monitoring results 12. the municipal, provincial or federal authorities that were notified of the situation or event 13. an indication of when and/or if further information will be submitted for the situation or event to the CNSC 14. for event reports of a contravention of a licence, licensees are to include a description of the nature of the non-compliance with the licence condition Detailed Event Reports shall contain the following information as far as practicable and applicable:	

Industry-Specific Requirements					
Requirement	**Reporting Threshold**	**Timing of Reporting**	**Method/Manner of Reporting**	**Content of Reporting**	**Penalties**
				1. reference to the original event report 2. updates, new or additional information on the content requirements of the event report 3. identification of any further missing information and the date that the missing information will be provided to the CNSC 4. the actions that the licensee has taken or proposes to take, including actions identified and taken to restore the effectiveness of the radiation or environmental protection programs 5. a description of the resulting effects on the health, safety and security of persons and the environment 6. the extent of condition or any review of a comparable situations or events 7. the measures taken to prevent recurrences 8. the effective dose and equivalent dose of radiation received by any person as a result of the situation or event, including the measured or estimated doses to NPP personnel and the public as a consequence of the situation or event 9. a summary of any analysis completed, including the probable cause(s) and conclusions, drawn from the investigation(s) after the situation or event 10. an evaluation of the degree of impairment of special safety systems or of standby safety-related systems 11. an evaluation of any design, operating and or training deficiencies uncovered by the situation or event	

Industry-Specific Requirements					
Requirement	**Reporting Threshold**	**Timing of Reporting**	**Method/Manner of Reporting**	**Content of Reporting**	**Penalties**
Ontario *Child, Youth and Family Services Act, 2017*, s. 308(2); O. Reg. 191/18, s. 8	Subject to any prescribed exceptions and additional requirements, if personal information that has been collected for the purpose of providing a service and that is in a service provider's custody or control is stolen or lost or if it is used or disclosed without authority, the service provider shall, a) notify the individual to whom the information relates at the first reasonable opportunity of the theft, loss or unauthorized use or disclosure; and b) include in the notice a statement that the individual is entitled to make a complaint to the Commissioner under section 316. (s 308(2)) If the circumstances surrounding the theft, loss or unauthorized use or disclosure meet the prescribed requirements, the service provider shall notify the Commissioner and the Minister of the theft, loss or unauthorized use or disclosure. (s 308(3)) Prescribed requirements: 1. The service provider has reasonable grounds to believe that the personal information was used or disclosed without authority by a person who knew or ought to have known that	Notify the individual to whom the information relates at the first reasonable opportunity of the theft, loss or unauthorized use or disclosure; and (s 308(2)(a)) • "as soon as reasonably practical" – OIPC Ontario guidance document	Breach reports can be submitted to the OIPC Ontario by mail or online.	Notify the individual to whom the information relates at the first reasonable opportunity of the theft, loss or unauthorized use or disclosure; and (b) include in the notice a statement that the individual is entitled to make a complaint to the Commissioner under section 316. (s 308(a)(b)) You will need to describe: • the circumstances of the breach (for example, how the personal information came to be stolen, lost, or disclosed without authority, how many individuals were affected, how the breach was discovered) • whether and how you notified the affected individuals • the nature of the personal information that was stolen, lost, or used or disclosed without authority • the steps you took to contain, investigate, and remediate the breach and prevent future breaches (some of this work may still be ongoing) • contact information of an employee who can provide additional information their right to complain to the OIPC Ontario	A person is guilty of an offence if the person..(f) wilfully fails to comply with clause 308(2)(a) (s 332(f)) A person who is guilty of an offence under subsection (1) is liable, on conviction, to a fine of not more than $5,000. (s 332(2)) If a corporation commits an offence under this Part, every officer, member, employee or agent of the corporation who authorized the offence, or who had the authority to prevent the offence from being committed but knowingly refrained from doing so, is a party to and guilty of the offence and is liable, on conviction, to the penalty for the offence, whether or not the corporation has

Industry-Specific Requirements					
Requirement	**Reporting Threshold**	**Timing of Reporting**	**Method/Manner of Reporting**	**Content of Reporting**	**Penalties**
	the person was using or disclosing the information without authority. 2. The service provider has reasonable grounds to believe that the personal information was stolen. 3. The service provider has reasonable grounds to believe that the personal information that was stolen or lost or used or disclosed without authority was or will be further used or disclosed without authority. 4. The loss or unauthorized use or disclosure of the personal information is part of a pattern of similar losses or unauthorized uses or disclosures of personal information in the custody or control of the service provider. 5. The service provider has reasonable grounds to believe that personal information that the service provider disclosed, to a prescribed entity or a person or entity that is not a prescribed entity under subsection 293 (1), (2) or (3) of the Act, has been stolen or lost or used or disclosed without authority by the prescribed entity or the person or entity that is not a prescribed entity.				been prosecuted or convicted. (s 332(3))

Industry-Specific Requirements					
Requirement	**Reporting Threshold**	**Timing of Reporting**	**Method/Manner of Reporting**	**Content of Reporting**	**Penalties**
	6. An employee of the service provider is terminated, suspended or disciplined as the result of the theft, loss or unauthorized use or disclosure of personal information by the employee. 7. An employee of the service provider resigns and the service provider has reasonable grounds to believe that the resignation is related to an investigation or other action by the service provider with respect to the theft, loss or unauthorized use or disclosure of personal information by the employee. 8. The service provider determines that the loss or unauthorized use or disclosure of the personal information is significant after considering all relevant circumstances, including, i. the sensitivity of the personal information that was lost or used or disclosed without authority, ii. the volume of the personal information that was lost or used or disclosed without authority, iii. the number of persons whose personal information was lost or				

Industry-Specific Requirements					
Requirement	**Reporting Threshold**	**Timing of Reporting**	**Method/Manner of Reporting**	**Content of Reporting**	**Penalties**
	used or disclosed without authority, and whether one or more service providers were involved in the loss or unauthorized use or disclosure of the personal information.				
Regulation respecting the management and reporting of information security incidents by certain financial institutions and by credit assessment agents, issued under the Quebec *Credit Assessment Agents Act, Insurers Act, Act respecting financial services cooperatives, Deposit Institutions and Deposit*	Where an information security incident with potentially adverse impacts is reported to the officers or managers of a financial institution or a credit assessment agent, the financial institution or the credit assessment agent must notify the Autorité des marchés financiers ("AMF") of the incident. "Information security incident" means an attack on the availability, integrity or confidentiality of information systems or the information they contain. The financial institution or the credit assessment agent must also notify the AMF of any information security incident that has been reported or been the subject of a notice to a regulatory body, a person or a body responsible under law for the prevention, detection or repression of crime or statutory offences or contractually responsible for providing compensation for injury that may have been caused by the incident. Where a financial institution or a credit assessment agent notifies the Commission d'accès à l'information of a confidentiality	The financial institution or the credit assessment agent must notify the Authority of the incident no later than 24 hours from the time the incident is reported. A financial institution or a credit assessment agent must notify the Authority of developments in the situation not later than three days after notice is given to the Authority and not later than every three days thereafter, until a notice is sent to the Authority	A financial institution or a credit assessment agent shall notify the Authority of an information security incident by completing the form available on the Authority's website.	The report confirming the incident is under control shall, in particular: (1) identify the source of the incident and the type of incident; (2) provide the financial institution's or credit assessment agent's assessment regarding a potential recurrence of the incident; and (3) describe the actions taken to reduce the likelihood of incidents of a similar nature occurring in the future. A financial institution or a credit assessment agent must maintain a current information security incident register that shall include, for each incident: (1) the date and time of the incident; (2) the location of the incident; (3) the nature of the incident; (4) a detailed description of the incident, including the information specified in subparagraph 2 of the report above; (5) any injury caused by the incident; (6) any third parties involved in the incident;	A monetary administrative penalty of $250 in the case of a natural person and $1,000 in any other case may be imposed on a financial institution or a credit assessment agent for failing to comply with reporting requirements; moreover, there may be a monetary administrative penalty of $500 in the case of a natural person and $2,500 in any other case imposed on a financial institution or a credit assessment agent that: (1) fails to develop or implement an information security

Industry-Specific Requirements					
Requirement	**Reporting Threshold**	**Timing of Reporting**	**Method/Manner of Reporting**	**Content of Reporting**	**Penalties**
Protection Act, Trust Companies and Savings Companies Act	incident referred to in paragraph 2 of section 3.5 of the Act respecting the protection of personal information in the private sector (chapter P-39.1), it must notify the Authority of the incident at the same time.	confirming that the incident is under control and that operations have returned to normal. A financial institution or a credit assessment agent shall send a report to the Authority within 30 days following the date the notice is sent to the Authority confirming that the incident is under control and that operations have returned to normal.		(7) actions taken; (8) whether the residual risk is accepted or not accepted and the rationale for accepting or not accepting it; (9) planned actions; and (10) the incident close date. A financial institution or a credit assessment agent must keep the information recorded in the register in a secure and confidential manner so as to maintain the information's integrity for a minimum period of five years from the date of the report.	incident management policy; (2) fails to maintain a current information security incident register; or (3) fails to keep the information in the information security incident register for a minimum period of five years from the date of the report.