March 31, 2023

Via Email: Caroline.Blouin@fsrao.ca

Caroline Blouin
Executive Vice President, Pensions
Financial Services Regulatory Authority of Ontario
25 Sheppard Ave W. Suite 100
Toronto, ON M2N 6S2

Dear Ms. Blouin:

We are writing on behalf of the administrators of the Health Care of Ontario Pension Plan ("**HOOPP**"), Ontario Teachers' Pension Plan ("**Ontario Teachers**"), OMERS Primary Pension Plan ("**OMERS**"), Colleges of Applied Arts and Technology Pension Plan ("**CAAT**") and OPSEU Pension Plan Trust Fund ("**OPTRUST**"). Collectively, we administer and manage the pension benefits of over 1.4 million members, with $518.3 billion in net assets under management. We submit this letter in response to the current consultation by the Financial Services Regulatory Authority of Ontario ("**FSRA**") regarding proposed guidance on Information Technology ("**IT**") Risk Management ("**Proposed Guidance**"). We appreciate the opportunity to review and comment on the Proposed Guidance and FSRA's approach to collaborative and cooperative engagement with regulated pension plans.

Overview

Prudent pension plan management requires administrators to manage a variety of risks, including those related to the use of IT. Plan administrators rely on information technology, whether through self-developed systems or third-party providers, for a variety of reasons including day-to-day administration systems and member engagement/communications. We take information management and the protection of member data seriously and we make our submissions with a view to the best interests of our plan members. Our interest as plan administrators is to ensure that regulation is consistent, appropriate for the pension sector, does not undermine existing security practices, and does not create undue burden.

In order to promote consistency, avoid confusion and leverage existing harmonized policy work completed by the Canadian Association of Pension Supervisory Authorities ("**CAPSA**"), in the context of the pension sector, we suggest that FSRA consider consulting on adopting the draft CAPSA Guideline on Cyber Risk for Pension Plans (the "**Draft CAPSA Guidance**") once it is finalized rather than developing additional separate guidance. Alternatively, if some form of FSRA guidance is maintained related to IT risk management, we agree that flexibility ought to be maintained to achieve the desired outcomes in a manner suitable for each plan based on its individual circumstances. We believe that consistent, principles-based guidance would be most effective and would support FSRA in achieving its statutory objects in the pension sector. To that end, we suggest that FSRA revisit the proposed guidance to ensure consistency with CAPSA, and clarify that it is information guidance in alignment to established regulatory practice in the pension sector. We have elaborated further on these with more granular comments below.

Consistency with CAPSA

CAPSA recently released Draft CAPSA Guidance that is tailored to the pension sector, which promotes a best practices approach to managing IT risks and incidents. The Draft CAPSA Guidance deals with the same subject as the Proposed Guidance. Given the Draft CAPSA guidance and the desire for consistency in the pension sector, FSRA should wait for the Draft CAPSA Guidance to be finalized – an approach other regulators, like OSFI, are taking – and adopt the Draft CAPSA Guidance for the Ontario pension sector. Proceeding with separate guidance introduces uncertainty for the sector, particularly given the differences between the Proposed Guidance and the Draft CAPSA Guidance, which are discussed in the following section.

Minimizing challenges of applying the guidance

If some form of FSRA guidance is maintained for the pension sector, we recommend that FSRA reconsider specific aspects of the Proposed Guidance, including the incident reporting framework, in order to better harmonize with CAPSA and minimize potential challenges of complying with the guidance.

The incident reporting framework contemplated by the Proposed Guidance may introduce challenges for plan administrators in the following areas:

- **Confidentiality** - The Proposed Guidance contemplates that administrators may provide FSRA with information about material incidents, including recovery and prevention plans, and states that FSRA will maintain confidentiality of any incidents reported by regulated entities and individuals to the extent allowed by law. However, under the PBA and other applicable legislation, FSRA may not be able to maintain confidentiality of the reported information. This information may be potentially discoverable through Freedom of Information requests or access requests from specified pension stakeholders who have information rights under the PBA. Reporting to FSRA under the current statutory framework could result in disclosure of sensitive business information that could reveal system vulnerabilities and remediation plans, to the detriment of the security of member information and business records. Immediate reporting to FSRA, and related engagement, may not align with other plan administrator obligations, for example where there has been a direction not to disclose information during a criminal investigation. We encourage FSRA to consider a framework for the pension sector that is sensitive to the unique confidentiality considerations related to reporting under the applicable statutory framework.

- **Timing of reporting** - Following an incident, administrators may have existing breach notification obligations to various stakeholders (members, vendors, regulatory bodies, and other 3rd parties) based on contractual, fiduciary, and/or other statutory or regulatory obligations. Immediate reporting of material incidents to FSRA followed by the regulatory engagement protocol contemplated by the Proposed Guidance may impede an administrator's ability to dedicate specialized resources to managing an incident and any mandatory reporting requirements. A more flexible direction regarding timing of notification would be necessary to ensure a practical application.

- **Determining materiality** - We agree that what constitutes a material incident is to be determined by the regulated entity. With that said, the reporting framework lists a variety of scenarios as indicators that a material incident has occurred. Given the varied nature of plans and the entities that offer plans, materiality should be sufficiently flexible such that recognition is given to the diversity of pension plans/administrators in Ontario. This diversity includes factors such as their individual approaches to their cyber and/or privacy programs, governance and internal reporting structures, risk appetite thresholds, and the nature of their cyber insurance policy. Materiality thresholds should be sufficiently high to ensure that only significant incidents with potential to materially impact the administrator's ability to fulfil its obligations to its members are reportable. We would question the value of reporting information where there is no impact to benefit security or the safety of plan member information, and note that doing so has the potential to consume both plan and regulator resources.

In addition, aspects of the guidance pose other challenges:

- **Commentary regarding breach of s. 22 and 30.1(2)** – Currently, the Proposed Guidance states that failure to follow the Practices for Effective IT Risk Management will likely result in a breach of ss. 22(1) and 30.1(2) of the PBA. We do not believe this to be a correct statement. First, s. 30.1(2) sets out requirements related to documents required to be sent under the PBA, regulations or FSRA rules. The failure to follow risk management practices may not impact documents delivered under s. 30.1 at all. Similarly, delivery of documents in accordance with s. 30.1 is not *per se* an indicator of sound IT risk management practices. In addition, a decision not to follow certain practices set out in the Proposed Guidance, which is described as information guidance and not set out in legislation, does not, in and of itself, establish a breach of section 22(1) of the PBA, particularly where there is no resulting harm, and where considerations such as confidentiality could dictate a different and more prudent course. In each case, the outcome will be dependent on the facts. Prejudging the circumstances or an administrator's decision-making in such hypothetical situations makes it more challenging for plan administrators to effectively respond to such scenarios.

Conclusion

FSRA's FY22-23 Statement of Priorities for the pension sector highlights the need for "appropriate principles-based and outcomes-focused implementation of the regulatory framework." In-line with that goal, and to promote greater regulatory consistency, we recommend that FSRA adopt the Draft CAPSA Guidance, rather than proceed with applying the Proposed Guidance to Ontario pension plans. Alternatively, if some form of FSRA specific guidance is maintained, we ask FSRA to revisit the Proposed Guidance from a principles-based perspective with a view to clarifying that it is best practices guidance, and implementing the other suggested revisions outlined above.

We would be happy to discuss our submission with you or answer any questions you may have on the above. Thank you for the opportunity to provide comments in response to this consultation.

Yours truly,

Saskia Goedhart
Chief Risk Officer
Healthcare of Ontario Pension Plan

Rossana Di Lieto
Senior Managing Director & Deputy Chief Legal Officer
Ontario Teachers' Pension Plan

Rodney Hill
Chief Risk Officer
OMERS Administration Corporation

David Gordon
Director, Public Affairs & Policy Projects
Colleges of Applied Arts and Technology Pension Plan

Dani Goraichy
Chief Risk Officer and Senior Vice President Actuarial Services
OPSEU Pension Plan Trust Fund

Saskia Goedhart
Chief Risk Officer
Healthcare of Ontario Pension Plan

Rossana Di Lieto
Senior Managing Director & Deputy Chief Legal Officer
Ontario Teachers' Pension Plan

Rodney Hill
Chief Risk Officer
OMERS Administration Corporation

David Gordon
Director, Public Affairs & Policy Projects
Colleges of Applied Arts and Technology Pension Plan

Dani Goraichy
Chief Risk Officer and Senior Vice President Actuarial Services
OPSEU Pension Plan Trust Fund

_____

Saskia Goedhart
Chief Risk Officer
Healthcare of Ontario Pension Plan

_____

Rossana Di Lieto
Senior Managing Director & Deputy Chief Legal Officer
Ontario Teachers' Pension Plan

Gareth Gibbins On behalf of

_____

Rodney Hill
Chief Risk Officer
OMERS Administration Corporation

_____

David Gordon
Director, Public Affairs & Policy Projects
Colleges of Applied Arts and Technology Pension Plan

_____

Dani Goraichy
Chief Risk Officer and Senior Vice President Actuarial Services
OPSEU Pension Plan Trust Fund

_____

Saskia Goedhart
Chief Risk Officer
Healthcare of Ontario Pension Plan

_____

Rossana Di Lieto
Senior Managing Director & Deputy Chief Legal Officer
Ontario Teachers' Pension Plan

_____

Rodney Hill
Chief Risk Officer
OMERS Administration Corporation

_____

David Gordon
Director, Public Affairs & Policy Projects
Colleges of Applied Arts and Technology Pension Plan

_____

Dani Goraichy
Chief Risk Officer and Senior Vice President Actuarial Services
OPSEU Pension Plan Trust Fund

_____

Saskia Goedhart
Chief Risk Officer
Healthcare of Ontario Pension Plan

_____

Rossana Di Lieto
Senior Managing Director & Deputy Chief Legal Officer
Ontario Teachers' Pension Plan

_____

Rodney Hill
Chief Risk Officer
OMERS Administration Corporation

_____

David Gordon
Director, Public Affairs & Policy Projects
Colleges of Applied Arts and Technology Pension Plan

_____

Dani Goraichy
Chief Risk Officer and Senior Vice President Actuarial Services
OPSEU Pension Plan Trust Fund