For Immediate Release
July 15, 2026

CSA publishes updated cybersecurity findings and guidance for registered firms

TORONTO – Today, the Canadian Securities Administrators (CSA) published CSA Staff Notice 33-322 *Review of Registered Firms' Cybersecurity Practices and Additional Guidance*. The Notice follows a focused compliance examination sweep of 73 registered firms' cybersecurity practices and sets out observed practices, identified gaps, and updated guidance to support firms in strengthening their cybersecurity frameworks.

The examinations covered a range of areas, including cybersecurity policies and procedures, employee training, risk assessments and controls, oversight of third-party service providers and incident response planning.

Overall, the CSA found that a number of firms examined, particularly larger firms, had robust cybersecurity policies and procedures. However, the CSA also identified gaps where firms could strengthen their cybersecurity practices. Compliance feedback has been provided to relevant firms for them to address the findings. In addition, the notice aims to provide practical, scalable guidance to firms of all sizes – including small and medium-sized firms – recognizing that cybersecurity risks and resources vary across registrants.

"The CSA wants to be clear with registrants that strong cybersecurity practices are not optional in today's threat environment. Our guidance is intended to help firms establish and maintain cybersecurity practices that are appropriate to their size and operations, and are responsive to an evolving threat landscape," said Stan Magidson, CSA Chair and Chair and CEO of the Alberta Securities Commission. "Cybersecurity risks continue to grow on many fronts, particularly as firms rely more heavily on digital tools, hybrid work arrangements and online platforms to serve clients. We expect firms to review this guidance, assess their own cybersecurity practices, identify any gaps, and take proactive steps to address them. While our examinations found that many registered firms have cybersecurity frameworks in place, they also identified areas where some firms could strengthen their practices."

Staff expect firms to have robust cybersecurity practices relevant to the firm's business. Registered firms are encouraged to review the notice and assess whether their cybersecurity practices can be strengthened, considering their current operations.

The CSA, the council of the securities regulators of Canada's provinces and territories, coordinates and harmonizes regulation for the Canadian capital markets.

Notes for editors:

- Registered firms' cybersecurity practices are assessed by CSA staff as part of compliance examinations conducted under section 11.1 of National Instrument 31-103 *Registration Requirements, Exemptions and Ongoing Registrant Obligations*.
- The Notice builds on CSA Staff Notice 33-321 *Cyber Security and Social Media* published in 2017 and reflects observations and guidance stemming from the recent CSA cybersecurity compliance examination sweep.

For media inquiries, please contact:

Curtis Lindsay
Ontario Securities Commission
media@acvm-csa.ca

Ilana Kelemen
Canadian Securities Administrators
media@acvm-csa.ca

For investor inquiries, please contact your local securities regulator.