Connecting Today.
Powering Tomorrow.

Independent Electricity System Operator
1600-120 Adelaide Street West
Toronto, ON M5H 1T1
t 416.967.7474
www.ieso.ca

Memorandum

To: **Stakeholder Advisory Committee**

From: Alex Foord, Chief Information Officer and Vice President, Information and Technology Services

Date: September 21, 2022

Re: IESO Business Update – Cyber Security

The following provides an update to members of the Stakeholder Advisory Committee (SAC) on the IESO's Cyber Security efforts.

The IESO was the first system operator in North America to be accountable for providing cyber security-related services to the broader electricity sector. This led to the creation of "Lighthouse" which is the cornerstone of the IESO's security offerings, providing a near real-time view into the threats and incidents that can impact the power grid. This detection, assessment and information-sharing service is the result of a one-of-a-kind partnership with the Canadian Centre for Cyber Security.

Through this initiative, the IESO is the centralized cyber security situational awareness and information exchange body for Ontario's licensed distribution and transmission companies. Entities that chose to participate in the cyber security services that the IESO provides are able to better position themselves in obtaining information about cyber security threats that may pose a risk to their organization and Ontario's electricity sector. The IESO works with the sector through various forms of engagement, such as surveys and working groups, to continue to develop and evolve IESO's cyber security services.

The IESO also regularly engages with federal and international partners to observe, monitor, and coordinate cyber security efforts and responses to material threats that may come forward.

Continuous monitoring is taking place on threats to the Ontario electricity sector and geo-political tensions between Russia and Ukraine. Continued cyber campaigns against Ukrainian organizations, including utilities, have been observed. Russian-affiliated threat actors have been reported as performing cyber-attacks against Ukrainian organizations using unique variants of sophisticated malware. This malware has not yet been observed outside of Ukraine. IESO has observed a nominal increase in scanning and reconnaissance activity since January 2022. In

Ontario, no incidents with material impact have been reported to or observed by the IESO that are attributable to Russian state-sponsored groups.

The IESO will continue to work closely with sector partners to emphasize its cyber security initiatives and will continue to prioritize this work. The recently refreshed IESO Corporate Strategy includes "Champion cyber security, situational awareness and best practices within the sector" as a key area of focus. The 2023-2025 IESO Business Plan also discusses the IESO's cyber security efforts, including cyber security considerations as part of the IESO's risk analysis and performance measures. Additional information on this can be found in the SAC memo on the IESO Business Plan.