Q. **Reference Application, Capital Programs and Projects, Install Intelligent Electronic Devices Management Software (2026–2028), page 1**

It is stated *"This manual process limits the amount of cybersecurity management that can be applied to the devices. This increases Hydro's cybersecurity vulnerability at a time when cyberattacks on electrical grid infrastructure are continually increasing in complexity and impact."*

a) How does a manual process increase cybersecurity risks?

b) In the event of a cyber attack, will Hydro have the ability to override the IED management software and manually control its assets?

A. **a)** Cybersecurity management involves frequent access to intelligent electronic devices to implement policies such as password management, monitoring for changes to security baseline, security patch management, security log management, and change management activities. Access frequency may range from monthly to yearly per policy per device. Given that Newfoundland and Labrador Hydro ("Hydro") has hundreds of intelligent electronic devices, completing this process manually would be very labor-intensive and in some cases require in-person field visits for devices, leading to longer processing times, creating a greater opportunity for cybersecurity risks.

b) Yes, products that Hydro has reviewed include the means to revert to manual control if required. This will be listed as a mandatory requirement when Hydro goes to tender for a solution.