**NEWS RELEASE**
**For immediate release**
**February 19, 2025**

**Commissioner's investigation calls for the Nova Scotia Government to take action to prevent future privacy breaches**

HALIFAX – On June 4, 2023, the Nova Scotia Government publicly announced it was subject to a global cyber security attack. Threat actors took advantage of a critical vulnerability in a software product called MOVEit, a file transfer system purchased and used by the Nova Scotia Government designed to move large amounts of data over the internet between users of the system. A vast scope of personal information, including names, social insurance numbers, addresses, educational backgrounds, personal health information and banking information was stolen by the threat actors that conducted the cyberattack.

In response to 110 complaints made by Nova Scotians whose privacy was breached by the cyberattack, Information and Privacy Commissioner Tricia Ralph launched an investigation into this matter.

In the Office of the Information and Privacy Commissioner for Nova Scotia (OIPC) investigation report issued today (*IR25-01*), Commissioner Ralph finds that the Nova Scotia Government failed to comply with its legal obligation to have reasonable security and information practices in place prior to its launching of the MOVEit file transfer system and during its use. Basic practices, such as completing a privacy impact assessment (a tool to identify privacy risks of a system) and having retention/disposition schedules, were not implemented. Commissioner Ralph found that this significantly exacerbated the extent and impacts of the privacy breach. She calls on the Nova Scotia Government to strengthen its security safeguards in order to protect Nova Scotians' personal information from the increasing threat of cyberattacks.

Commissioner Ralph also finds that while the Nova Scotia Government took reasonable steps to contain the privacy breach, notified affected individuals in a timely manner, and offered an appropriate length of time for credit monitoring, there were also shortcomings in the Nova Scotia Government's actions in response to the breach. These shortcomings and the Commissioner's recommendations to address them include:

- The privacy breach notification letters and call centre staff tasked with responding to inquiries by affected individuals provided insufficient information regarding the privacy breach. This unnecessarily added to the stress and worry that affected individuals went through when they received their breach notification letters. The Commissioner recommends that in future, the Nova Scotia Government seek input from the OIPC before issuing privacy breach notification letters to individuals.

- In many cases, the contact information used in the breach notification letters was very outdated. This meant that thousands of affected individuals did not receive notification that they were entitled to and so were unable to take measures to protect themselves. The Commissioner recommends that the Nova Scotia Government takes steps to ensure that it has up-to-date contact information for all citizens that it holds personal information about.
- The Nova Scotia Government's response plan is insufficient. It lacks transparency and accountability. The Commissioner recommends that the Nova Scotia Government make its plan public and update the public on its implementation.

Overall, Commissioner Ralph makes 8 recommendations to the Nova Scotia Government for follow-up actions and to strengthen its security safeguards in order to protect Nova Scotian's personal information from the increasing threat of cyberattacks. The Nova Scotia Government is considering the report and will have 30 days to formally decide whether it will follow Commissioner Ralph's recommendations.

Commissioner Ralph states that, "Nova Scotians have the right to know whether the public institutions that collect and use their personal information utilize systems that are secure and defensible from cyberattacks. This is why it is so important for the Nova Scotia Government to be proactive and continuously review and update its security and information practices to stay ahead of ever-evolving threat actors. The increasing number of cyberattacks does not mean that we as citizens are forced to throw our expectation of privacy out the window. It means that we, as citizens, must demand more of the public institutions that collect personal information about us. Real leadership at the highest level in the Nova Scotia Government is needed to ensure that adequate security and information practices, which are required by law, are implemented."

-30-

Media contact:
Jason Mighton
Senior Investigator
902-424-4684
oipcns@novascotia.ca