Office of the Information & Privacy Commissioner
Nova Scotia

NEWS RELEASE
For immediate release
January 15, 2019

Privacy Commissioner's investigation determines that a serious failure of due diligence led to Freedom of Information Access website privacy breaches

HALIFAX – Information and Privacy Commissioner Catherine Tully issued her investigation report today into a series of privacy breaches that plagued the Freedom of Information Access (FOIA) website in the spring of 2018. The Commissioner determines that the immediate cause of the privacy breaches was a design flaw in the FOIA website. The flaw was created by a well-known and foreseeable vulnerability that was not detected by the Department of Internal Services (Department) prior to launching the FOIA website. Ultimately, the privacy breaches were preventable and were caused by a serious failure of due diligence in the deployment of a new technology tool.

The privacy breaches occurred between February 27, 2018 and April 3, 2018. The investigation confirmed that a total of almost 7000 records containing personal information were downloaded by two individuals in a series of 12 privacy breaches. More than 600 of those records have not yet been located.

The investigation identified shortcomings in the project management, security review and privacy impact assessment processes that resulted in the implementation of the FOIA website with more than two dozen vulnerabilities unidentified and unmitigated. One of those vulnerabilities resulted in the privacy breaches that were the subject of the Privacy Commissioner's investigation.

"Taking the time to diligently assess a tool at all stages of a project, before deployment, is fundamental to ensuring that personal information held by government is respected and protected," Tully said.

Following discovery of the privacy breaches, the Department undertook a process to manage the privacy breaches. Overall, the Privacy Commissioner concludes that the Department's breach management was insufficient. The Commissioner determines that the breaches have not been contained, notification of affected individuals was inadequate and overall the Department lacks a comprehensive and methodical plan to prevent a similar occurrence in the future.

The law requires public bodies such as the Department to make reasonable security arrangements to protect personal information. In this case, the Department failed to meet this statutory requirement. The Commissioner makes six recommendations to the Department aimed at

strengthening its privacy program and identifying and remedying security vulnerabilities that may be affecting other collections of personal information currently held by government.

The Department has accepted all six recommendations.

“There are two critically important changes that must occur if privacy is to be truly protected and respected. First, there is a need for strong leadership, leadership that is committed to significant change and meaningful implementation of the recommendations. Second, there must be an evolution of the role of my office and fundamental changes to our outdated legislation,” said the Commissioner.

As a result, the Commissioner has again written to the Premier to recommend essential improvements to Nova Scotia’s privacy laws.

The investigation report and the letter to the Premier is available on the Office of the Information and Privacy Commissioner for Nova Scotia’s website at https://oipc.novascotia.ca/.

The Auditor General also issued a separate report on the same privacy breaches today. His work can be found at www.oag-ns.ca.

-30-

Media contact:

Janet Burt-Gerrans, Senior Investigator
Phone: 902-424-4684
Email: oipcns@novascotia.ca
Twitter: @NSInfoPrivacy

BACKGROUNDER
January 15, 2019

About the Information and Privacy Commissioner for Nova Scotia
The Information and Privacy Commissioner for Nova Scotia is appointed as the impartial oversight authority under the *Freedom of Information and Protection of Privacy Act* and the *Privacy Review Officer Act.*

Freedom of Information and Protection of Privacy Act
The *Freedom of Information and Protection of Privacy Act* (*FOIPOP*) applies to all "public bodies" as defined in *FOIPOP* s. 3(1)(j). The Department of Internal Services is a public body subject to the *FOIPOP* access and privacy rules. *FOIPOP* sets rules around protection of personal information that all public bodies must follow. Section 24(3) says, "The head of the public body shall protect personal information by making reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure or disposal."

Jurisdiction to investigate
Pursuant to s. 5(1)(b) of the *Privacy Review Officer Act,* the Privacy Commissioner initiated an investigation into a series of privacy breaches that involved the Department of Internal Services' website known as the Freedom of Information Access website (FOIA website).

Investigative process
The Commissioner initiated this investigation following receipt of a breach notification from the Department of Internal Services (Department) on April 9, 2018. Investigators reviewed a wide range of documents including policies, contracts, meeting minutes, inventory of records, website activity logs and project charters. Twenty government employees were interviewed representing all aspects of the development, procurement, implementation and operation of the FOIA website. Investigators also interviewed representatives of the Halifax Regional Police, the government employee who alerted the Department to the issue, staff from Saint Mary's University, the Atlantic School of Theology and four different website users individually affected by the breaches.

What are the key findings of this investigation report?
The immediate cause of the privacy breaches was a design flaw in the FOIA website. This flaw created a well-known and foreseeable vulnerability that was not detected by the Department prior to launching the FOIA website. Ultimately, this series of privacy breaches was preventable and was caused by a serious failure of due diligence in the deployment of a new technology tool.

As part of responding to this series of privacy breaches, an independent security firm conducted a full security assessment. That assessment revealed more than two dozen other vulnerabilities in the FOIA website system that the Department was unaware of.

This investigation identified shortcomings in the project management, security review and privacy impact assessment (PIA) process that resulted in the implementation of the FOIA website with these vulnerabilities. Those shortcomings included:

- The Department incorrectly rated the risks as low based at least in part on the trusted relationship with the vendors. This relationship inspired a sense that the projects were low risk which permeated all aspects of the project development and deployment.
- The project management process and user testing did not incorporate any technical testing and failed to recognize the risk associated with the storage database design – specifically the storage of public and private documents in the same database.
- The short time frames created a stressful environment and compromised the quality of system testing.
- The Department failed to act on information that there were risks associated with the lack of website vulnerability scanning.
- The Department failed to complete a timely and specific security threat and risk assessment after the clear recommendation to do so from Department Cyber Security staff and the Information and Privacy Commissioner.
- The privacy impact assessment process was neither diligent nor rigorous.
- The Department relied on one vendor for technical security measures included in the PIA instead of conducting its own analysis.
- The Department failed to incorporate risks and mitigations identified during the project into the PIA.

In summary, the processes lacked due diligence. Risk assessments lacked rigor, at times not going beyond passive acceptance of untested conclusions or unverified claims nor beyond blind trust in vendor claims. The *Freedom of Information and Protection of Privacy Act* requires that public bodies make reasonable security arrangements to protect personal information. The Department failed to make reasonable security arrangements for the FOIA website as required by s. 24(3) of *FOIPOP*.

Following discovery of the privacy breaches, the Department undertook a process to manage the privacy breaches. This process must also satisfy the reasonable security requirements of *FOIPOP*. With respect to the privacy breach management undertaken by the Department, the key findings in this report include:

- The Department's initial containment action of shutting down the website was reasonable but the breaches are not contained. More than 600 documents containing personal information were downloaded onto an unknown computer and have not yet been recovered or secured.
- The Department's initial notification efforts were reasonable and timely. However, there are an unknown number of third parties affected by the download of the 600 plus documents who have not been notified.
- The Department lacks a comprehensive, methodical plan to prevent a similar occurrence in the future.

What are the recommendations arising from this report?
The Commissioner makes six recommendations to the Department of Internal Services:

1. Strengthen privacy leadership in government and due diligence in the privacy impact assessment process.
2. Take immediate steps to contain the breaches that resulted in the download of 618 documents containing personal information to a private computer that has not been secured by the Department (breaches #2 - #12).
3. Take all reasonable steps necessary to notify individuals affected by the download of the 618 documents containing personal information (breaches #2 - #12).
4. Conduct an internal post-incident review as an aid to ensuring that the Department fully understands the causes of these breaches and has identified all reasonable steps necessary to prevent future similar errors.
5. Conduct an inventory of technology solutions, devices and applications across government and rate their vulnerabilities. From there create a plan to mitigate cyber security vulnerabilities beginning with systems storing the most vulnerable personal information and/or having the highest risk.
6. Clarify and strengthen the role of the Architecture Review Board.