Nova Scotia Post Incident Response Final Status Report for the MOVEit File Transfer Service

Department of Cyber Security and Digital Solutions

February 19, 2026

Introduction

In response to Recommendation 8 of the Office of the Information and Privacy Commissioner (OIPC) for Nova Scotia Investigation Report concerning the MOVEit system privacy breach, this report includes a final overview of and status report on the Government of Nova Scotia's post incident response plan concerning this event. Per the OIPC report the Government of Nova Scotia has re-framed its recommendations as mandatory requirements. All recommendations have been completed or remain an ongoing activity beyond the scope of this report.

Report Scope

As required by the Nova Scotia [Privacy Breach Protocol](#), the Government of Nova Scotia prepared an internal privacy breach report which included a series of recommendations specific to the MOVEit breach. They were formulated through the investigative process of the Privacy Breach Protocol and through consultation with staff members actively engaged in identifying and responding to the breach. A public version of the report can be found on the MOVEit breach [website](#).

This publication makes these recommendations public and provides a status update on each item. The recommendations are organized into the following three areas of improvement:

- MOVEit Secure File Transfer Service: recommendations to enhance the security of the MOVEit system and the supporting business processes.

- Breach Protocol and Incident Response: recommendations to increase the resiliency and response to large-scale breaches.

- Data Governance Practices: recommendations to enhance data governance practices.

Interdepartmental teams have been collaborating across departments, public bodies and with other partners such as NSH and IWK to implement these recommendations. They continue to collaborate on privacy matters.

Status of OIPC MOVEit Investigation Recommendations Implementation

#	Recommendation	Accept (Y/N)	Completion Timeline	Status	Date or Target Date for Completion	Accountable Department
1	Complete PIA of MOVEit file transfer system.	Y	Within 60 days	Complete	7 March, 2025	Cyber Security and Digital Solutions (CSDS)
2	Make appropriate sections of PIA publicly available on website.	Y	Within 60 days	Complete	23 April, 2025	CSDS
3	Create clear retention and disposition schedules for all users of MOVEit that specifies maximum amount of time files can remain in repository of MOVEit.	Y	Within 60 days	Complete	4 March, 2025	CSDS
4	Commit to ensuring retention and disposition schedules are adhered to by monitoring system on annual basis, if not more frequently.	Y	N/A	Complete	4 March, 2025	CSDS
5	Confirm commitment to consult with OIPC in advance of notification letters for future major privacy breaches.	Y	Within 60 days	Complete	8 April, 2025	Service Nova Scotia (SNS)
6	Make every reasonable effort to ensure government has up-to-date contact information for all citizens that it holds personal information about.	Y	N/A	Ongoing	Ongoing priority.	Government of Nova Scotia
7	Complete and post on website a comprehensive post incident response plan: • Makes all recommendations of government's internal report mandatory. • Sets timelines and deadlines for all activities related to the same recommendations. • Sets accountability at Ministerial level for implementation of the tasks/activities. • Addresses concerns raised and recommendations of OIPC investigation.	Y	Within 90 days	Complete	16 May, 2025	CSDS
8	Complete tasks/activities of the post incident response plan and post results to website within 1 year.	Y	Within 1 year	Complete	19 February, 2026	CSDS

Status of Post Incident Response Plan Implementation

Internal Report Requirement Category	Internal Report Requirements	Accountable Department	Status	Target Date for Completion	OIPC Report Recommendation Alignment
MOVEit Secure File Transfer Service	Apply data access control for users.	CSDS	Complete	19 May, 2025	Recommendations 3, 4
	Develop processes or guidelines for appropriate data use.	CSDS	Complete	4 March, 2025	Recommendations 3, 4, 5
	Implement additional safeguards for MOVEit and services that use the application.	CSDS	Complete	4 March, 2025	Recommendations 3, 4, 5, 6
	Improve user awareness of the application.	CSDS	Complete	4 March, 2025	Recommendations 3, 4
Breach Protocol and Incident Response	Review and adapt the existing privacy breach protocol for a large-scale breach or extensive compromise of security that results in unauthorized access to a substantial amount of sensitive or confidential information.	SNS	Complete	4 March, 2025	Recommendations 3, 4, 5, 6
	Review and enhance the existing cyber security incident response process.	CSDS	Complete	4 March, 2025	Recommendations 3, 4, 5, 6
Data Governance	Communicate the applicability of existing formalized data classification framework(s) to accurately categorize data based on sensitivity.	CSDS	Complete	3 April, 2024	Recommendations 3, 4, 5, 6
	Establish a data retention policy for the government that outlines requirements for data management and disposition throughout the data lifecycle.	CSDS	Complete	4 March, 2025	Recommendation 3, 4