Office of the Information and Privacy Commissioner for Nova Scotia

INVESTIGATION REPORT IR25-01

MOVEit File Transfer System Privacy Breach

Tricia Ralph
Information and Privacy Commissioner for Nova Scotia

TABLE OF CONTENTS

Office of the Information and Privacy Commissioner for Nova Scotia
Report of the Commissioner (Review Officer)
Tricia Ralph

INVESTIGATION REPORT IR25-01

February 19, 2025

Nova Scotia Government

Commissioner's Message

Cyber security attacks (cyberattacks) are becoming more common as we move through the digital age. Does that mean they are inevitable and so we must learn to abandon our right to privacy and accept that it can no longer be protected? Of course not. What it means is that public institutions who collect and use personal information about its citizens need to work harder to prevent future cyberattacks. It means that governments need to be more vigilant and continuously update their security and information measures to keep up with the evolving sophistication of threat actors.

In 2023, the Nova Scotia Government, as well as its Nova Scotia Health (NSH) and Izaak Walton Killam (IWK) Health partners (collectively referred to as Nova Scotia Government) were subject to, by far, the biggest cyberattack of its kind ever experienced in this province. Threat actors exploited a vulnerability in a file transfer system used by the Nova Scotia Government called MOVEit to exfiltrate vast amounts of personal information about thousands of Nova Scotians. Privacy breach notification letters were sent to approximately 168,000 individuals. Those affected ranged from current and former Nova Scotia Government employees (including job applicants) to members of the public, youth, incarcerated individuals and more. While not everyone had the same type of personal information stolen, the variety of types of personal information that was stolen was considerable. It included things like financial information, social insurance numbers, contact information, personal health information, and more. Most of the information stolen is extremely sensitive and its misuse could have significant ramifications on those affected for many years down the road.

The Office of the Information and Privacy Commissioner for Nova Scotia (OIPC)'s investigation into this matter revealed that at the time of the cyberattack, the Nova Scotia Government failed to comply with its obligation to have reasonable security and information safeguards in place. In my view, this considerably exacerbated the impacts of the privacy breach. Much of the personal information stolen would not have been accessible to steal had the Nova Scotia Government had additional safeguards in place prior to the MOVEit cyberattack. I recommend that the Nova Scotia Government strengthen its security and information practices for its use of the MOVEit

file transfer system, namely complete a privacy impact assessment and create retention/disposition schedules for MOVEit.

In terms of its response to the cyberattack, the OIPC's investigation determined that the Nova Scotia Government took reasonable steps to contain the breach once it became aware of it, notified affected individuals in a timely manner and offered an appropriate length of time for credit monitoring. These steps were important because the OIPC's investigation revealed that the harms from this breach were significant and foreseeable. However, the Nova Scotia Government's post-containment approach has room for improvement. I recommend that the Nova Scotia Government create a mandatory and comprehensive post-incident response plan. I also recommend that it make this plan publicly available and update the public as to its implementation. A prevention plan becomes meaningless if it is not implemented. Transparency is key to holding the Nova Scotia Government accountable for ensuring that the lessons learned from this cyberattack can be used to prevent and better respond to future breaches.

One of the biggest lessons to be learned from this experience is that the Nova Scotia Government should make greater efforts to properly resource itself and the OIPC. In terms of resourcing issues at the OIPC, the average amount of privacy complaints that the OIPC receives in a given year is 10. The OIPC received 110 privacy complaints in one year about the MOVEit cyberattack. In 2022 the OIPC received 820 calls from the public on *all matters* related to the OIPC. In 2023, the OIPC received 700 calls from affected individuals *solely in relation to MOVEit*. Despite the Nove Scotia Government being aware that the OIPC already had a significant backlog of cases at the time of the MOVEit cyberattack and despite the significant amount of work that responding to the cyberattack required from the OIPC, the Nova Scotia Government did not provide the OIPC with any additional resources to respond to the MOVEit privacy breach. This is troubling. It is time to acknowledge and address the impacts that not adequately resourcing the OIPC has. I urge the Nova Scotia Government to adequately resource the OIPC. I ask it to put serious thought into what the purpose of having an oversight office is if that office is denied the resources it needs to fulfill its role in a timely manner.

In terms of adequately resourcing itself, the Nova Scotia Government explained in its response to the OIPC that a contributing factor that made its response to this privacy breach challenging was that there was a lack of resources in various teams to support a breach response of this scale and complexity. I have no doubt that the staff working to prevent and rectify this cyberattack did the best with what they had. The critical commentary contained in this report is directed solely at leadership. Again, I urge the Nova Scotia Government to adequately resource itself so that it has sufficient resources to prevent and respond to future cyberattacks.

My hope is that the Nova Scotia Government responds to this matter by showing real leadership. In addition to the resourcing issue, real leadership is demonstrated by accepting and implementing the recommendations set out in this report. 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.

Tricia Ralph
Information and Privacy Commissioner for Nova Scotia

Executive Summary

[1] On June 4, 2023, the Nova Scotia Government publicly announced it was subject to a global cyber security attack (cyberattack).[1] Threat actors took advantage of a critical vulnerability in a software product called MOVEit. MOVEit is a file transfer system purchased and used by the Nova Scotia Government. It is designed to move large amounts of data over the internet between users of the system.

[2] This breach impacted an estimated 18.5 million people worldwide.[2] It is unclear exactly how many individuals were affected by the Nova Scotia Government's use of MOVEit, however approximately 168,000 privacy breach notification letters were sent to individuals identified as victims of this breach.

[3] A vast scope of personal information, including names, social insurance numbers, addresses, educational backgrounds, personal health information and financial information was stolen by the threat actors that conducted the cyberattack.

[4] The Office of the Information and Privacy Commissioner for Nova Scotia (OIPC)'s investigation finds that, while the Nova Scotia Government took reasonable steps to contain the privacy breach, there were shortcomings in the implementation and use of the MOVEit file transfer system, as well as in the Nova Scotia Government's actions in response to the breach.

[5] In terms of the shortcomings in the implementation and use of MOVEit, overall, this investigation found that the Nova Scotia Government failed to have reasonable security and information practices in place as required by the *Freedom of Information and Protection of Privacy Act* (*FOIPOP*) and the *Personal Health Information Act* (*PHIA*). The Nova Scotia Government did not conduct a privacy impact assessment (PIA) on the MOVEit file transfer system. A PIA is an essential safeguard used to identify risks to privacy of a given project or program. Had a PIA been conducted when the MOVEit system was acquired, it is probable that many of the shortcomings or misuses of the MOVEit file transfer service identified in the OIPC's investigation could have been identified and addressed. This may have lessened the impact of the breach. As such, I recommend that a PIA be completed within 60 days.

[6] The Nova Scotia Government also frequently misused the MOVEit file transfer system as a repository for personal information. It also did not create retention/disposition schedules that specified the maximum amount of time that files being transferred within the MOVEit file

[1] Nova Scotia Government, *Global Privacy Breach Impacts Nova Scotia* (June 4, 2023), online: Cyber Security and Digital Solutions <https://news.novascotia.ca/en/2023/06/04/global-privacy-breach-impacts-nova-scotia>.
[2] Nova Scotia Government, *The Cyber Security Attack on Nova Scotia's MOVEit System, Public Report* (May 2024), online: https://novascotia.ca/privacy-breach/docs/cyber-security-attack-moveit-public-report.pdf, at p. 1. Note this Investigation Report addresses only the breach in Nova Scotia.

transfer system could remain in the repository of MOVEit. This is a basic security and information practice that was not followed. This misuse of the MOVEit file transfer system as a repository for storing personal information greatly exacerbated the extent of the privacy breach. Had there been retention/disposition schedules that users were required to follow, the MOVEit file transfer system would not have been misused in this way. And as a result, much of the personal information would not have been available to the threat actors that stole it. To that end, I recommend that the Nova Scotia Government formulate retention/disposition schedules and take measures to ensure they are followed.

[7] Although the OIPC's investigation found that the Nova Scotia Government took reasonable steps to contain the breach and quickly notified affected individuals, there were some shortcomings in the Nova Scotia Government's actions in response to the breach. These shortcomings and my 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. For this reason, I recommend that in future, the Nova Scotia Government consult with the OIPC prior to deployment of privacy breach notification letters to affected individuals on major privacy breaches so that the OIPC can provide suggestions to address any deficiencies in breach notification letters.
- 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. I recommend that the Nova Scotia Government make every reasonable effort to ensure that it has up-to-date contact information for all citizens that it holds personal information about.
- While the Nova Scotia Government did create recommendations to itself following its own investigation to prevent a similar future breach, it did not create a clear and thorough post-incident response plan. I recommend that a more comprehensive and mandatory plan be created and made public and the Nova Scotia Government update the public on its implementation.

[8] When the Nova Scotia Government issued its public report on its investigation of the MOVEit cyberattack, the then Minister of Cyber Security and Digital Solutions Minister Colton LeBlanc said: "I'd love to be able to say we will never face another cybersecurity breach. Cyberthreats are unfortunately a reality in the world we now live in. Everyone – governments, private companies and people – are all at risk. We must take steps to protect ourselves…"[3] I agree. Cyberattacks are likely to continue and are likely to become more and more sophisticated as threat actors attempt to steal information from the Nova Scotia Government. That is why prevention is so key. Real leadership is required to ensure that the Nova Scotia Government stays ahead of these attempts.

[3] Nova Scotia Government, *News release: MOVEit Public Report Released* (May 29, 2024), online: Department of Cybersecurity and Digital Solutions <https://news.novascotia.ca/en/2024/05/29/moveit-public-report-released>.

1.0 BACKGROUND

[9] Progress Software Corporation® (the vendor) is an entity that provides various software products for purchase. One of the software products it offers is called MOVEit®. The MOVEit software is meant to empower entities to "[T]ake control of their file transfer workflows with solutions that help secure, simplify and centralize data exchanges throughout the organization."[4] The MOVEit software essentially acts as a file transfer service that facilitates the exchange of digital information. It is designed to do so in a secure manner.

[10] The MOVEit system transfers files within the MOVEit transfer module using one of two methods: (1) ad hoc secure email transfer (i.e., log-in, attach a file, and send it), or (2) automated (i.e., scheduled) file transfer. The Nova Scotia Government, Nova Scotia Health (NSH), and Izaak Walton Killam (IWK) Health use both methods to facilitate the exchange of digital information within government, public bodies, and external organizations and partners. File transfer systems are meant to be used to transfer information, not as a repository to store information. Once the information has been transferred, it should be removed from the system. There are typically retention schedules that specify how long information can be kept in the repository before it must be removed.

[11] On May 31, 2023, the vendor identified a critical vulnerability in its MOVEit file transfer software that allowed remote attackers to gain unauthorized access to the MOVEit transfer database and posted information about this vulnerability on its website. The vendor reported that the vulnerability in the MOVEit transfer module could lead to escalated privileges and potential unauthorized access to the environment; meaning data could be stolen.[5]

[12] IBM X-Force, a third party on retainer with the Nova Scotia Government to provide cyber security incident response services, later confirmed that data was stolen from the Nova Scotia Government's MOVEit file sharing service on May 30 and 31, 2023.

[13] On June 1, 2023, the Nova Scotia Government declared a major incident[6] and initiated its privacy breach protocol. This included taking the MOVEit system offline and installing the updates recommended by the vendor.

[14] On June 3, 2023, the Department of Cyber Security and Digital Solutions (CSDS) confirmed data was stolen from the Nova Scotia Government's MOVEit system. Specifically, data was stolen only through the automated file transfer function of the MOVEit file transfer system; no information in the ad hoc secure email transfer function was stolen. Threat actors exploited the vulnerability, gaining administrative access (i.e., full access to content in the file share repository and control of the system) to the MOVEit system. After gaining access, the threat actors downloaded files that were held in the repository of the MOVEit file transfer

[4] Progress, *Managed Files Transfer Software* (undated), online: <https://www.progress.com/moveit.
[5] Progress Community, *MOVEit Transfer Critical Vulnerability (May 2023) (CVE-2023-34362)* (June 16, 2023), online: <https://community.progress.com/s/article/MOVEit-Transfer-Critical-Vulnerability-31May2023.
[6] Nova Scotia Government, *Privacy breach alerts and information* (August 3, 2023), online: <https://novascotia.ca/privacy-breach/>.

system, including files containing personal information and personal health information of citizens and employees.[7]

[15] The Nova Scotia Government notified the Office of the Information and Privacy Commissioner for Nova Scotia (OIPC) of the cyber security attack on June 4, 2023.

[16] Between late June 2023 and September 2023, approximately 168,000 privacy breach notification letters were sent to affected individuals from four entities: the Department of Cyber Security and Digital Solutions (CSDS), the Department of Health and Wellness (DHW), Nova Scotia Health (NSH) and Izaak Walton Killam (IWK) Health.

[17] The population of affected individuals included thousands of active and former Nova Scotia Government employees. A vast scope of personal information, including names, social insurance numbers, addresses, educational backgrounds and banking information was stolen.

2.0 JURISDICTION AND INVESTIGATIVE PROCESS

2.1 Jurisdiction

[18] The OIPC provides independent oversight of the *Freedom of Information and Protection of Privacy Act (FOIPOP),* the *Personal Health Information Act (PHIA)*, and the *Privacy Review Officer Act (PRO),* as well as related regulations. The OIPC has the authority to investigate privacy complaints under section 5(1)(b) of *PRO* and section 92(2)(b) of *PHIA*. As an oversight body, the OIPC has a mandate to assess the level of compliance with the law, to make recommendations where appropriate, to advocate for best practice and to assist public bodies and custodians in establishing effective privacy management programs.

[19] In this case, public bodies under the jurisdiction of *FOIPOP* and custodians under the jurisdiction of *PHIA* were affected. *FOIPOP* applies to "public bodies" which it defines as a "Government department or a board, commission, foundation, agency, tribunal, association or other body of persons;"[8] *PHIA* applies to "custodians" which are defined as "an individual or organization described below who has custody or control of personal health information as a result of or in connection with performing the person's or organization's powers or duties."[9]

[20] In other words, depending on the personal information stolen, an entity can be subject to the oversight provisions of *PRO* (for non-health personal information) or *PHIA* (for personal health information).

[21] The OIPC received approximately 110 privacy complaints under *PRO, FOIPOP* and *PHIA* as a result of individuals being notified that their privacy had been breached due to the MOVEit incident. The OIPC decided to launch an own-motion investigation with each of the four above noted entities, in order to collectively respond to these privacy complaints in one report. To

[7] Nova Scotia Government, *The Cyber Security Attack on Nova Scotia's MOVEit System Public Report* (May 2024), online: <https://novascotia.ca/privacy-breach/docs/cyber-security-attack-moveit-public-report.pdf>.
[8] *FOIPOP*, s. 3(1).
[9] *PHIA*, s. 3.

address this significant volume and any systemic issues, the own-motion investigation was launched under *PRO, FOIPOP* and *PHIA.*

[22] *FOIPOP* and *PHIA* both contain privacy and security provisions. Section 24(3) of *FOIPOP* requires that public bodies make reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure or disposal. Sections 61, 62 and 65 of *PHIA* set out the security standards expected of custodians. *PHIA* provides a more detailed and higher expectation of security than *FOIPOP*, especially with regards to maintaining an electronic information system. For this reason, my analysis in this report will apply the more rigorous security standards provided in *PHIA* to all entities: CSDS, DHW, NSH and IWK Health (collectively referred to as the "Nova Scotia Government" in this report).

2.2 Investigative process

[23] The Department of Cyber Security and Digital Solutions (CSDS) "[I]s responsible for maintaining and transforming information technology operations for the Province and the health sector."[10] It manages the MOVEit file transfer service for all Nova Scotia Government users including DHW, NSH and IWK Health. When the OIPC initiated this investigation, all four entities were given the opportunity to provide their responses to us. However, each chose to allow the Nova Scotia Government to reply on its behalf. Despite having individual, and at times different obligations under their relevant legislation, these organizations declined to represent themselves and instead informed the OIPC that their responses would be incorporated into CSDS' responses to the OIPC. For this reason, and because CSDS is responsible for maintaining technology operations for all Nova Scotia Government departments and the health sector, and because CSDS is a department of the Nova Scotia Government, the findings and recommendations in this report are directed to the Nova Scotia Government. It is up to the Nova Scotia Government to ensure that all its departments and health sector partners implement the recommendations herein.

[24] On April 3, 2024, the OIPC requested the Nova Scotia Government's privacy breach report, its cyber security report and any supporting documents.

[25] In response, on April 18, 2024, the Nova Scotia Government provided the OIPC with its report into the cyberattack titled *Nova Scotia Privacy Breach Protocol, Privacy Breach Report, MOVEit File Transfer Service* (*Privacy Breach Report*) on behalf of CSDS, DHW, NSH and IWK Health. Based on information within that report, the OIPC made a follow-up request for supporting documents that were referenced but not provided with the *Privacy Breach Report*. On July 24, 2024, CSDS followed up with additional records and, where documents were unavailable or not included, explanations and/or context.

[26] The OIPC did not conduct interviews; my findings and recommendations are based on the OIPC investigation team's research, input from affected individuals who made complaints to the OIPC and the responses provided by the Nova Scotia Government.

[10] Nova Scotia Government, *New Department to Focus on Digital Services, Programs* (May 24, 2023), online: <https://news.novascotia.ca/en/2023/05/24/new-department-focus-digital-services-programs>.

[27] This investigation did not specifically address technical aspects of the breach, as the OIPC was not provided with staff or funding from the Nova Scotia Government to conduct such an analysis. This is unfortunate, as this report may have benefited from such expertise.

[28] For a report on the state of the Nova Scotia Government's cyber security readiness, readers may wish to review the Office of the Nova Scotia Auditor General's 2024 *Report on Cybersecurity Readiness in Healthcare*,[11] which also references the MOVEit breach.

3.0 ISSUES

[29] There are four issues in this investigation:

1. Did a privacy breach occur?
2. What was the cause of the privacy breach?
3. Did the public body have reasonable security and information practices in place for its use of the MOVEit file transfer system as required by s. 24(3) of *FOIPOP* and ss. 61, 62 and 65 of *PHIA*?
4. Did the public body take reasonable steps in response to the reported privacy breach as required by s. 24(3) of *FOIPOP* and ss. 61 and 62 of *PHIA*?

4.0 ANALYSIS & FINDINGS

4.1 Issue #1: Did a privacy breach occur?

[30] A privacy breach occurs when personal information is collected, used, and/or disclosed without authority under the relevant legislation, which in this case is *FOIPOP* and *PHIA*. A privacy breach can also occur when a public body/custodian has not adequately safeguarded personal health information.[12]

[31] In this case, the Nova Scotia Government reported the incident as a privacy breach to the OIPC. Personal information was exfiltrated through the MOVEit system. There is no doubt that a privacy breach occurred.

[32] **Finding #1:** I find that a privacy breach occurred.

4.2 Issue #2: What was the cause of the privacy breach?

[33] Before I can assess whether or not the Nova Scotia Government made reasonable security and information arrangements for its use of the MOVEit file transfer system, it is first important to understand the technical cause of the privacy breach.

[34] Based on the OIPC's investigation, the root cause of the breach was essentially technical. Threat actors gained unauthorized access to the MOVEit file transfer system by exploiting a

---

[11] Office of the Auditor General of Nova Scotia, *Cybersecurity Readiness in* Healthcare (October 22, 2024), online: <https://oag-ns.ca/sites/default/files/2024-10/Interactive%202024%20Cybersecurity%20Readiness%20in%20Healthcare.pdf>.

[12] *SK Investigation Report 136-2024, 169-2024, 183-2024, 187-2024, 191-2024*, *Innomar Strategies Inc. (Re)*, 2024 CanLII 116817 (SK IPC), at para. 24.

zero-day vulnerability[13] in the MOVEit software. After gaining access, the threat actors downloaded files residing within the MOVEit repository.

[35] **Finding #2:** I find that the root cause of the breach was that threat actors exploited a critical vulnerability in the MOVEit file transfer system and used it to gain access to the personal information that was stored in the MOVEit repository.

4.3 Issue #3: Did the public body have reasonable security and information practices in place for its use of the MOVEit file transfer system as required by s. 24(3) of *FOIPOP* and ss. 61, 62 and 65 of *PHIA*?

[36] Section 24(3) of *FOIPOP* provides that the head of a public body must protect personal information by making reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure or disposal.

[37] Sections 61, 62 and 65 of *PHIA* set out the security standards expected of custodians. *PHIA* requires that custodians protect the confidentiality of personal health information and that they do so by implementing information practices[14] (such as policies) that are reasonable in the circumstances. Section 65 requires additional safeguards for custodians who maintain an electronic information system by requiring the custodians to implement additional safeguards as set out in the *Personal Health Information Regulations,* such as implementing safeguards that ensure only those authorized to access electronic information systems have access.[15]

[38] The meaning of "reasonable security" in Nova Scotia's privacy laws has been canvassed by the OIPC on several occasions.[16] Factors to consider when evaluating the reasonableness of an entity's security include: the sensitivity of the information, ensuring that security measures are not technically or operationally prescriptive, the foreseeability of a privacy breach, impacts on trust of the entity, industry standards, cost, life cycle of records, format of the records, ability to nimbly respond to risks and documentation of procedures.

---

[13] A zero-day vulnerability is a software vulnerability that is not yet known by the vendor, and therefore has not been mitigated. A zero-day exploit is an attack directed at a zero-day vulnerability. See: Canadian Centre for Cyber Security, *Glossary* (undated), online: <https://www.cyber.gc.ca/en/glossary#z>.

[14] Information practices are defined in s. 3 of *PHIA* as:

"information practices", in relation to a custodian or a prescribed entity, means the policies of the custodian or a prescribed entity for actions in relation to personal health information, including

> (i) when, how and the purposes for which the custodian routinely collects, uses, discloses, retains, de-identifies, destroys or disposes of personal health information, and
>
> (ii) the administrative, technical and physical safeguards and practices that the custodian maintains with respect to the information;

[15] *Personal Health Information Regulations,* NS Reg 217/2012, at s. 10.

[16] *NS Report IR17-01, Cape Breton-Victoria Regional School Board (Re)*, 2017 NSOIPC 9 (CanLII); and *NS Report IR16-02, Nova Scotia Health Authority and Private Practice Physicians (Re)*, 2016 NSOIPC 16 (CanLII) for example. In both reports, former Commissioner Tully noted that the summary of considerations supplied above are consistent with every other jurisdiction in Canada. The issue was further canvassed in *NS Report IR18-01, Department of Health and Wellness (Re),* 2018 NSOIPC 12 (CanLII), *NS Report IR18-02, Sobeys National Pharmacy Group (Re),* 2018 NSOIPC 13 (CanLII), *NS Report IR19-01, Department of Internal Services (Re),* 2019 NSOIPC 2 (CanLII); and *NS Review Report 20-02, Nova Scotia Health Authority (Re),* 2020 NSOIPC 2 (CanLII).

[39] When assessing whether the Nova Scotia Government had reasonable security and information arrangements in place for its use of the MOVEit file transfer system, it is important to assess whether there were any unmitigated issues that may have contributed to the breach and its impacts.

[40] Overall, our investigation found two major shortcomings that led me to find that the Nova Scotia Government did not have reasonable security and information practices in place for its use of the MOVEit file transfer system. The first was that it failed to complete a privacy impact assessment (PIA) and the second was that it did not create retention/disposition schedules for information being transferred and/or stored in the MOVEit system.

The privacy impact assessment process

[41] A central piece of any privacy program is a PIA. Privacy impact assessments are a common administrative safeguard utilized to identify privacy risks of a given project or program. Modern privacy laws make the completion of PIAs in advance of implementing a new project or system mandatory. Even in jurisdictions without a mandatory statutory requirement, like here in Nova Scotia, PIAs are often mandated by government policy and are always recommended by privacy commissioners.[17]

[42] Best practice is to consider the PIA process as an evergreen process. This means that PIAs are completed in stages beginning with the conceptual stage of a new or changed program or system. Conducting a PIA is a red flag exercise that identifies potential issues very early in a proposed project or system. If the project proceeds, then the PIA is expanded to the design stage and the privacy risks are evaluated and mitigation strategies identified. Before implementation, the PIA must be reviewed to ensure that risks identified have indeed been mitigated and to identify any new risks that may have emerged. PIAs should also include a review schedule that requires privacy leads to revisit the project periodically to ensure that any new or emerging risks are properly identified and mitigated.[18]

[43] The Nova Scotia Government told the OIPC that it implemented a privacy policy in 2008 (*2008 Privacy Policy*). This version is no longer available online. It was updated to the current privacy policy in 2018 (*2018 Privacy Policy*). [19] These policies mandate that PIAs be completed in certain circumstances.

[44] As part of this investigation, the OIPC asked for the Nova Scotia Government's PIA on its use of the MOVEit system. In response, the Nova Scotia Government explained that it had not done a PIA for MOVEit. It said that its partnership with the vendor began in 2006, prior to the implementation of the *2008 Privacy Policy*, which would have required that a PIA be completed. It said that it did not go back and conduct a PIA for MOVEit after the implementation of the *2008 Privacy Policy*. In addition, when the *2018 Privacy Policy* was implemented (approximately five years before the MOVEit breach), the Nova Scotia Government similarly did not go back and conduct a PIA for MOVEit. The result is that by the time of the cyberattack,

---

[17] *NS Investigation Report 19-01, Department of Internal Services (Re),* 2019 NSOIPC 2 (CanLII), at para. 81.
[18] *NS Investigation Report 19-01, Department of Internal Services (Re),* 2019 NSOIPC 2 (CanLII), at para. 82.
[19] Nova Scotia Government, *4.II Privacy Policy* (May 8, 2018), online: <https://www.novascotia.ca/treasuryboard/manuals/PDF/300/30411-04.pdf> [*2018 Privacy Policy*]

the Nova Scotia Government's use of the MOVEit file transfer system had never been compliant with the *2008 Privacy Policy* nor the *2018 Privacy Policy*. A PIA for MOVEit was never completed.

[45] Considering the volume and sensitivity of the personal information housed in the MOVEit system, this was a serious oversight. The fact that the Nova Scotia Government began using MOVEit prior to the implementation of the *2008 Privacy Policy* does not excuse it from the requirement to retroactively conduct a PIA. An updated policy or practice must apply to the information held *at that time*, not just the information collected *after that date*. It must apply to the systems currently being used.

[46] Had the Nova Scotia Government conducted a PIA prior to the use of the MOVEit file transfer system or when the privacy policy was adopted in 2008 and updated in 2018, many of the shortcomings or misuses of the MOVEit system could have been identified and addressed. Specifically, many records that were not appropriately stored on the system could have been moved to non-networked locations or disposed of in accordance with a standard retention policy. Had this information been removed from the MOVEit repository, it would not have been available to the threat actors.

[47] **Finding #3:** I find that by not conducting a PIA when it began its use of the MOVEit file transfer system or when the Nova Scotia Government's privacy policy was adopted in 2008 and updated in 2018, the Nova Scotia Government failed to have reasonable security and information practices in place and was therefore not in compliance with s. 24(3) of *FOIPOP* or ss. 61, 62 and 65 of *PHIA*.

[48] **Recommendation #1:** In August 2024, the Nova Scotia Government indicated that a PIA for MOVEit was being completed at that time. If this task is not yet finished, I recommend that the Nova Scotia Government complete a thorough and up-to-date PIA on its use of the MOVEit file transfer system within 60 days of the date of this report.

[49] **Recommendation #2:** I further recommend that, within 60 days of the date of this report, the Nova Scotia Government make the appropriate portions of the PIA on MOVEit publicly available on its website. Any portions of the PIA that could provide an opportunity for future exploitation by threat actors should not be reported publicly.

Retention and disposition schedules

[50] A fundamental component of robust security and information practices is the creation of and adherence to retention/disposition schedules. Employees should have access to written policies and procedures that detail a records retention and disposition schedule.

[51] MOVEit is a file transfer system. Once files have been transferred from one user to another, the files should be removed from the system's repository. The MOVEit system has a default retention period of 14 days for leaving information in the repository. Despite this, some users stored information in the repository of MOVEit for considerably longer than 14 days. The Nova Scotia Government explained that whether information was left in the repository for less or more than 14 days was based on users' decisions. No processes, guidelines or

retention/disposition schedules were set out by the Nova Scotia Government to ensure that the information was not stored in the repository for longer than it needed to be. This was a serious oversight, particularly given the nature and volume of the personal information that was contained in the system.

[52] The extent of the information breached was significantly compounded by the Nova Scotia Government's practice of retaining files in the MOVEit repository for longer than needed or required, rather than being removed from the repository once the files had been transferred and received.

[53] This practice of not having guidance on when information should be removed from the repository left volumes and volumes of data vulnerable to being stolen by the threat actors. It significantly exacerbated the extent of this breach. Simply put, had information been removed from the repository in accordance with reasonable retention/disposition schedules, it would not have been stolen. Overall, it is evident to me that the MOVEit file transfer system was, in many cases, overly misused as a repository rather than its intended file transfer purpose.

[54] **Finding #4:** I find that the MOVEit file transfer system was frequently and inappropriately used as a repository for extraneous records and that this exacerbated the extent of the personal information breached in the cyberattack.

[55] **Finding #5:** I find that the Nova Scotia Government did not provide sufficient direction to MOVEit users regarding the length of time that files should be kept in the repository of the MOVEit file transfer system and that this exacerbated the extent of the personal information breached in the cyberattack.

[56] **Recommendation #3:** I recommend that, within 60 days of the date of this report, the Nova Scotia Government create clear retention and disposition schedules for all users of the MOVEit file transfer system that specifies the maximum amount of time that files being transferred can remain in the repository of MOVEit.

[57] **Recommendation #4:** I further recommend that the Nova Scotia Government commit to ensuring that retention and disposition schedules are adhered to by monitoring use of the MOVEit system on a yearly basis, if not more frequently.

4.4 Issue #4: Did the public body take reasonable steps in response to the reported privacy breach as required by s. 24(3) of *FOIPOP* and ss. 61 and 62 of *PHIA*?

[58] The reasonableness of a response following a privacy breach must be assessed within the specific circumstances of the privacy breach. The OIPC encourages entities responding to a privacy breach to follow four steps, as set out in the OIPC's guidance document entitled *Key Steps to Responding to Privacy Breaches* (*NS OIPC Key Steps Document*).[20] The four key steps are:

1. Contain and investigate the breach
2. Evaluate the risks
3. Notification
4. Prevention

Step 1: Contain and investigate the breach

[59] Step 1 of the response to a privacy breach is to contain and investigate it. This step requires a custodian to take immediate and common-sense steps to limit the breach. The specific steps required will depend on the specific privacy breach at issue, but include:

a) *Contain:* Immediately stop the unauthorized practice and shut down a breached electronic information system or access to an electronic information system.
b) *Initial investigation:* Immediately conduct an initial investigation with a designated lead individual who has authority to complete the initial investigation. Conduct a more detailed investigation subsequently if required.
c) *Internal notifications:* Give appropriate internal notifications to the privacy officer and others who need to be made aware.
d) *Breach response team:* Determine whether a breach response team is required.
e) *Police*: Determine whether police should be involved.
f) *Preserve evidence:* Preserve any evidence of what occurred.[21]

[60] As set out in the *Privacy Breach Report*, The Nova Scotia Government's containment efforts included the actions in the timeline below.

June 1, 2023

[61] CSDS declared a major incident, established incident response coordination, took the MOVEit system off-line and applied the security updates recommended by the vendor to mitigate the potential risks. The major incident was downgraded by end of day June 1 and the service was restored on the same day.

[62] CSDS also received a priority notification from the Canadian Centre for Cyber Security (CCCS) indicating that the Nova Scotia Government may be using a version of the MOVEit software that contained a vulnerability that could be exploited. Patching had already been

[20] NS OIPC, *Key Steps to Responding to Privacy Breaches* (December 2019), online: NS OIPC <https://oipc.novascotia.ca/sites/default/files/publications/Key%20Steps%20to%20Responding%20to%20Privacy%20Breaches%20-%20OIPC%20-2019%2012%2002.pdf> [*NS OIPC Key Steps Document*].
[21] *NS OIPC Key Steps Document*, at p. 3.

completed on the MOVEit system and so this notification did not require further action by CSDS.

June 2, 2023

[63] CCCS contacted CSDS to recommend further investigation into suspicious internet protocol (IP) addresses. CSDS took the system off-line again and investigated and confirmed that the suspicious IP addresses were present in the environment.

[64] CSDS notified the Nova Scotia Government's Chief Information Access and Privacy (IAP) Officer.

[65] The CSDS technical team initiated a triage call with IBM X-Force, a third party on retainer with the Nova Scotia Government to provide cyber security incident response services, and requested that the X-Force team conduct a forensic analysis of the MOVEit system.

[66] CSDS followed the recommendations of IBM X-Force, vending partners, and internal system experts to determine if any data had been stolen and to ensure the system was secure.

June 3, 2023

[67] CSDS continued with its technical investigation to determine if any data was stolen. Executive leadership meetings were held with NSH and IWK Health executives and privacy leads, Communications Nova Scotia (CNS) and the Chief IAP Officer to raise their awareness of the issue.

[68] CSDS established workstreams to determine the service impact of having MOVEit off-line, service restoration timelines, technical remediation if needed, communications, and privacy (in collaboration with the Chief IAP Officer).

[69] CSDS contacted colleagues in other Canadian jurisdictions for advice and recommendations.

[70] IBM X-Force completed further analysis of the MOVEit system and confirmed that data had been stolen on May 30 and May 31, 2023.

[71] CCCS and IBM X-Force provided evidence that there was no indication of an operating system level breach or lateral movement to other end points with the government environment.

[72] CSDS, with support from IBM X-Force, confirmed no data had been taken since the patching activities on June 1.

[73] An initial list of compromised files was provided by CSDS to the privacy leads at NSH and IAP Services.

June 4, 2023

[74] Within 24 hours of confirmation that data had been stolen from the MOVEit system, CSDS and privacy specialists from impacted organizations began a detailed analysis of the data and

confirmed that files belonging to NSH, IWK Health, the Nova Scotia Government and its public sector partners were among the organizations whose data was compromised.

[75] CSDS contacted the CCCS to confirm a cyber security incident had occurred and that data was stolen.

[76] The Chief IAP Officer notified the OIPC that a privacy breach had occurred.

[77] CSDS contacted the Halifax Regional Police, and a police report was filed. A submission was also filed with the Canadian Anti-Fraud Centre (CAFC).

[78] The Nova Scotia Government issued a press release advising Nova Scotians that personal data had been breached and that further analysis was ongoing.[22]

[79] Meetings were held with executive leadership, workstream leads, privacy leads, and communications.

June 5, 2023
[80] CSDS confirmed MOVEit system stability. With the security updates in place, the executive team approved the recommendation from the technical team to resume use of the MOVEit system for users. Additional security updates and monitoring measures were also implemented at this time.

[81] CSDS communicated with internal departments and held several internal meetings to provide updates and coordinate the response effort.

June 6, 2023
[82] CSDS began full server restoration of the original MOVEit system that hosts the file share repository.

June 7, 2023
[83] CSDS discussed the breach at a departmental all-staff meeting and had a follow-up discussion with the Halifax Regional Police.

June 8, 2023
[84] CSDS held separate meetings with TransUnion to discuss credit monitoring services and Communications Nova Scotia to discuss the transition from cyber security incident response to privacy breach response. The Chief IAP Officer provided a status update to the OPIC.

June 9, 2023
[85] The vendor posted another critical MOVEit vulnerability which was flagged by CSDS staff monitoring the vendor's website and industry news sources. CSDS then assessed the vulnerability, applied a patch, performed a full version upgrade, and restored the MOVEit service.

---

[22] Nova Scotia Government, *Global Privacy Breach Impacts Nova Scotia* (June 4, 2023), online: Cyber Security and Digital Solutions <https://news.novascotia.ca/en/2023/06/04/global-privacy-breach-impacts-nova-scotia>.

June 15, 2023
[86] Another MOVEit vulnerability was posted by the vendor and flagged by CSDS staff monitoring the vendor's website and industry news sources. CSDS declared another major incident. CSDS blocked all user access to the MOVEit system.

June 16, 2023
[87] The MOVEit system was patched by CSDS, and service was restored. As part of ongoing maintenance, more patching occurred in the following weeks as the vendor identified new vulnerabilities.

[88] No files were compromised during the events of June 1 through June 16. The stolen files were taken between May 30 to 31, 2023.[23]

[89] **Finding #6:** I find that the Nova Scotia Government took reasonable steps to contain the privacy breach following its discovery. Specifically, the response was timely and engaged third-party cyber security experts who provided essential instructions.

Step 2: Evaluate the risks
[90] The second step in appropriately managing a privacy breach is to evaluate the risks. The purpose of this step is to ensure that the public body fully understands what took place and the extent of the identified risks to inform any further actions it may take. Evaluating the risks may lead to identifying additional containment steps or may point toward appropriate preventative strategies.

[91] To evaluate the risks, a public body must consider the nature of the personal information involved, the individuals affected, the cause and extent of the breach, and the foreseeable harm from the breach.[24]

Nature of the personal information involved
[92] The type of personal information involved is extensive and sensitive. It included things like:

- name, address, home phone number
- social insurance number
- healthcare card number
- pension payment amounts and pension recipients
- date of birth
- banking information
- salary information
- licence plate numbers

[23] Nova Scotia Government, *The Cyber Security Attack on Nova Scotia's MOVEit System Public Report* (May 2024), online: <https://novascotia.ca/privacy-breach/docs/cyber-security-attack-moveit-public-report.pdf>.
[24] *NS OIPC Key Steps Document* at p. 4-6.

Individuals affected

[93] Individuals who were affected by the breach included some:

- Past and present employees of regional centres for education and Conseil Scolaire Acadien provincial.
- Employees of Nova Scotia Health
- Employees of IWK Health
- Employees of the provincial public service
- People who applied for jobs with Nova Scotia Health
- People issued Halifax Regional Municipality parking tickets
- People in provincial adult correctional facilities
- Clients of the Department of Community Services[25]
- People in the Department of Health and Wellness client registry
- People in the Department of Health and Wellness provider registry
- Halifax Water customers
- Past and present certified teachers
- People involved with the Prescription Monitoring Program
- Newborns born between May 19 and 24, 2023
- Patients in the early labour and assessment unit at IWK Health

Cause and extent of the breach

[94] As detailed above, the cause of this breach was a focused cyberattack conducted by threat actors that exploited a zero-day vulnerability in the MOVEit software used by the Nova Scotia Government.

[95] The breach was extensive in terms of the sensitivity and diversity of the information breached and the number of individuals affected.

Foreseeable harm from the breach

[96] The Nova Scotia Government based its determination of risk of harm on a number of factors but focused primarily on whether the information could be used for identity theft. Considering the vast amount of identity attributes stolen and not recovered, including social insurance numbers, banking information and date of birth, I agree that the most immediate and foreseeable risks of harm from the privacy breach is identity theft, which could also result in extortion. However, there are two main other potential risks that the Nova Scotia Government failed to identify.

[97] First, there is also the potential for embarrassment or humiliation should an affected individual's personal information re-appear on the internet or in another public space.

[98] Second, there is also a foreseeable harm to public trust in the Nova Scotia Government's ability to safeguard sensitive personal information as a result of this breach.

[25] Since the time of the writing this report, the Department of Community Services is now called the Department of Opportunities and Social Development.

[99] Overall, the risks from this extensive breach involving some of the most sensitive and intimate personal information held by the Nova Scotia Government, are high. Data is easily stored long-term by threat actors and they may release individuals' information at any time, especially when individuals least expect them to do so. The Nova Scotia Government offered most affected individuals credit monitoring services for a period of five years at no charge. Although I find that the 5-year credit monitoring period is reasonable for this cyberattack, I do wish to put the Nova Scotia Government on notice that at least one Commissioner has recently recommended a 10-year credit monitoring period or longer in response to privacy breaches.[26] It is likely that the OIPC will consider recommending longer credit monitoring periods in future.

[100] **Finding #7:** I find that the harm from this privacy breach is significant and was foreseeable.

[101] **Finding #8:** I find that the 5-year credit monitoring offered to affected individuals by the Nova Scotia Government is reasonable.

Step 3: Notification

[102] The third step in managing a privacy breach is to determine whether privacy breach notification to affected individuals is appropriate and necessary. Section 69 of *PHIA* requires the custodian to notify an affected individual at the first reasonable opportunity if the custodian believes on a reasonable basis that, because of the breach, there is potential for harm or embarrassment to the individual. While *FOIPOP* does not require notification, it is undoubtedly best practice, especially in a criminal context like this where there is the possibility of identity theft. CSDS notified affected individuals even when *FOIPOP* did not mandate it to and that was, in my view, the right thing to do.

[103] Notification conveys respect to affected individuals and allows them to take steps to mitigate any potential harm. Former Information and Privacy Commissioner for Nova Scotia Catherine Tully said "best practices call for the notification letter to be specific and precise in describing the breach and its outcome to affected individuals. This shows respect for the affected individuals and informs their ability to take steps to mitigate potential harm."[27]

[104] According to the *Privacy Breach Report*, created by the Nova Scotia Government after the cyberattack, the Nova Scotia Government's notification process included the following measures:

1. Indirect notification began on June 4, 2023, through press releases, continuing media updates and a website. The Nova Scotia Government advised the public to monitor their banking information closely, watch for any suspicious transactions and proactively contact their banking institutions for additional security.
2. Direct privacy breach notification letters were sent to affected individuals from June 16 to the end of September 2023.

---

[26] *SK OIPC Investigation Report 136-2024, 169-2024, 183-2024, 191-2024, Innomar Strategies Inc. (Re), 2024* CanLII 116817 (SK IPC), at para. 38.
[27] *NS IR18-01, Department of Health and Wellness (Re)*, 2018 NSOIPC 12 (CanLII) at para. 145.

[105] Each affected department and custodian completed forms in which they listed the stolen files and produced a risk rating based on the sensitivity of the information and other factors. The Nova Scotia Government determined that individual privacy breach notification was appropriate for the affected persons in files rated high or medium risk. This determination was based on the type of information that had been breached, the extent of the breach and the risk of identity theft or fraud or other significant harms (such as sensitive personal health information). Individuals in some lower rated risk files also received notification where it was deemed to be appropriate. A number of individuals did not receive direct notification because the risk rating performed by the affected departments determined that the data elements could not be used by the threat actors to commit identity theft.

Timing

[106] Direct notification began on June 16, 2023, and the last letters were sent by the end of September 2023.

[107] *PHIA* requires notification at the "first reasonable opportunity" but that is the extent of its instruction in terms of timing. Guidelines and laws tend to be imprecise about time limits on notification because various circumstances must be accounted for. In that light, the reasonableness of the timing can be measured by whether it is objectively diligent and prudent in the circumstances.[28]

[108] Former Commissioner Tully canvassed what "first reasonable opportunity" means:

> The reasonableness of the timing is measured by whether it is objectively diligent and prudent in all the circumstances. Guidelines and laws tend to be imprecise with regard to time limits on notification to affected individuals because circumstances must be accounted for. Guidelines around notification in Canada suggest multiple formats for notification to affected individuals, always with the purpose of best facilitating the individual taking steps to mitigate harm. It is not necessary that each individual receive the same form letter notification after the investigation is complete. A public body can take a tailored approach to notification at multiple stages of the investigation if that would best facilitate mitigation of harm. For example, initial notification by phone call to provide the individual preliminary ability to manage the risks, followed by formalized notification later in the process, may provide the individual better opportunity to mitigate the potential damage caused by the breach. Typically, this is taken to mean within days or possibly weeks of identifying a breach, but not months.[29] The reasonableness of the time period can also be impacted by the circumstances. Best practices also acknowledge that if a police investigation is part of the containment strategy, this may weigh in favour of delaying notification to allow maximum opportunity for containment to be effective. A very high volume of records to be analyzed in order to identify affected individuals could also weigh in favour of some delay in order to accurately notify individuals.[30]

---

[28] *NS IR18-01, Department of Health and Wellness (Re),* 2018 NSOIPC 12 (CanLII), at para. 133.
[29] The European General Data Protection Regulation (GDPR) requires notification to oversight agencies within 72 hours and "without undue delay" to affected individuals. Numerous American notification laws require notification "immediately" but not later than 45 days.
[30] *NS IR19-01, Department of Internal Services (Re),* 2019 NSOIPC 2 (CanLII), at paras. 146-147.

[109] In this case, the extensive volume of information and affected individuals weighed in favour of an immediate public notification (indirect notification), which was done by the Nova Scotia Government. The phased stages of direct notification that followed, as well as the consistent updating of online and media information, were also appropriate measures. While the last direct notification letters were sent nearly four months after the breach, the level of resources and analysis required to execute direct notification was unprecedented.

[110] **Finding #9:** I find that the timing of the indirect and direct privacy breach notification to affected individuals was reasonable.

Accuracy and sufficiency of information provided in the notification

[111] The privacy breach notification letters informed affected individuals of the breach, the information impacted, the risk to themselves, steps taken by the Nova Scotia Government to contain the breach, steps the affected individuals could take to mitigate their own risk, contact information for further questions and contact information for the OIPC should the affected individuals want to file a privacy complaint with the OIPC. The letters set out the specific information elements that had been breached for each affected individual. However, in many cases, while the information element was noted, the granular piece of the information element was not made clear. For example, a notification letter would say that an email or phone number was stolen but did not specify whether the email and phone number was work or personal in nature.

[112] Soon after the first breach notification letters were sent, recipients began calling the OIPC. The most common complaints received were:

- The letter was addressed to a deceased relative.
- The letter was sent to an old address.
- Some of the granular pieces of the impacted information elements were vague.
- Regarding the breach itself, individuals wanted more information about the group responsible and if a ransom had been requested and paid.
- In trying to determine if the letter was legitimate, many callers searched online for the toll-free contact phone number provided by the Nova Scotia Government and information about CSDS but could not find either. This caused further unnecessary angst for the victims as they were unsure whether the breach notification letter itself was also an attempt to breach their privacy.
- Callers contacted the OIPC with the impression that the OIPC was CSDS and had information about the breach. Many stated that this was because the OIPC's phone number was the only local number on the letter, and that it was at the end of the letter.
- The toll-free telephone number provided for CSDS did not work outside of Nova Scotia.

[113] The Nova Scotia Government established a toll-free number service staffed by Service Nova Scotia's existing contact centre team to answer questions from affected individuals. While this was well intentioned, the dedicated phone line was actually a source of frustration for both affected individuals and the OIPC. I want to acknowledge that the Nova Scotia Government did appropriately refer affected individuals to the OIPC when they wanted to file a privacy complaint with the OIPC. However, things went awry when affected individuals called the OIPC with

general questions unrelated to filing a privacy complaint. The OIPC was frequently told by affected individuals that call centre representatives had told them that they could only "go over what was in the letter." Affected individuals also told the OIPC that when call centre staff could not respond to their non-privacy complaint related questions, call centre staff referred them to the OIPC. The Nova Scotia Government said that these types of callers with more complex non-privacy complaint related questions were referred to Nove Scotia Government privacy leads. The OIPC does not know whether Nova Scotia Government privacy leads or call centre staff were referring callers to the OIPC for non-privacy complaint related questions, but ultimately, an unacceptable number of callers with general questions were referred by the Nova Scotia Government to the OIPC. While the OIPC informed the Nova Scotia Government that callers should only be referred to the OIPC if they wanted to file a privacy complaint, the OIPC continued to receive questions about the breach months after the notification letters were sent.

[114] A practical way to address the issues that arose from the wording of the breach notification letters would have been to seek input from the OIPC prior to sending them to affected individuals so that the OIPC could give suggestions for improvement based on its past experiences. In this case, a copy of the template letter was provided to the OIPC, but it was not provided to the OIPC with enough time to incorporate the OIPC's suggestions in the first round of breach notification letters that were sent out. This meant that the first round of notification letters did not include suggested wording from the OIPC and this likely resulted in many more calls to the OIPC and the call centre than would have occurred if the notification letters had incorporated the OIPC's suggestions. Subsequent breach notification letters did incorporate many of the OIPC's suggestions. While I cannot be sure, I suspect that affected individuals who received the first iteration of the breach notification letter would have experienced less stress, made fewer calls and made fewer complaints, had they initially received the later version of the notification letter that incorporated suggestions from the OIPC.

[115] There were also issues with the contact information for affected individuals. Section 24(2) of *FOIPOP* requires that "where a public body uses an individual's personal information to make a decision that directly affects the individuals, the public body shall make every reasonable effort to ensure that the information is accurate and complete."[31] The *2018 Privacy Policy* requires that "government entities shall undertake reasonable efforts to ensure that all personal information held by the government entity, and which is to be used in any decision-making process affecting an individual, is as accurate, up-to-date and complete as possible."[32]

[116] One Nova Scotia Government department user of MOVEit explained that when it sent out notification letters to affected individuals, 14,200 letters were returned. It is clear from the amount of notification letters that were returned that the Nova Scotia Government used inaccurate and outdated information. While there are many reasons for this requirement of accurate information, it is an essential security measure to facilitate proper notification to affected individuals in the event of a privacy breach.

[117] **Finding #10:** I find that the notification letters and call centre staff provided insufficient information regarding the breach and the personal information impacted.

---

[31] *FOIPOP*, s. 24(2).
[32] *2018 Privacy Policy*, at p. 5.

[118] **Finding #11:** I find the contact information used for the notification letters was severely outdated in many cases. This meant that thousands of affected individuals did not receive notification letters and were unable to take measures to protect themselves.

[119] **Recommendation #5:** I recommend that, within 60 days of the date of this report, the Nova Scotia Government confirm a commitment to consult with the OIPC in advance of issuing privacy breach notification letters for future major privacy breaches in a manner that allows sufficient time for OIPC suggestions to be incorporated into the notification letters.

[120] **Recommendation #6:** I recommend that the Nova Scotia Government make every reasonable effort to ensure that it has up-to-date contact information for all citizens that it holds personal information about.

Step 4: Prevention

[121] The final step in managing a privacy breach required by the *NS OIPC Key Steps Document* is to work to prevent a future occurrence.

[122] To prevent a similar future privacy breach, it is essential for the Nova Scotia Government to understand the root causes of the breach and to evaluate the factors that contributed to it occurring. In accordance with my findings above, the immediate cause of the breach was the exploitation by threat actors of a critical vulnerability in the MOVEit system. Shortcomings in the privacy impact assessment process, lack of retention/disposition schedules, and improper use of the MOVEit repository function significantly increased the severity and extent of the impacts of the cyberattack.

[123] Best practice following a cyberattack is to conduct a comprehensive, reflective post-breach review and then develop a thorough prevention strategy that sets out concrete responsive actions.[33] With respect to personal health information, the *Personal Health Information Regulations* mandate custodians to keep a record of all corrective actions they take to reduce the likelihood of future breaches.[34] *FOIPOP* has not been substantively updated in over 30 years and so it does not have this requirement. Nevertheless, the Nova Scotia Government has a document titled *Managing a Privacy Breach Protocol and Forms* (*NSG Privacy Breach Protocol*)[35] that includes a post-incident review requirement. It states:

> Privacy breach investigations should be led by the privacy designate/IAP administrator with the support of the program/business area leadership. As required, other areas will be engaged such as security, HR, etc. The investigation will include a review of the business practices and procedures, access controls in place, security (physical and technical), and interviews with staff involved.[36]

---

[33] *NS IR19-01, Department of Internal Services (Re)*, 2019 NSOIPC 2 (CanLII), at para. 155.
[34] Section 10(4), *Personal Health Information Regulations*, NS Reg 217/2012.
[35] Nova Scotia Government, *Managing a Privacy Breach Protocol and Forms* (July 2017), online: Information Access and Privacy (IAP) Services <https://beta.novascotia.ca/sites/default/files/documents/1-1132/managing-privacy-breach-protocol-and-forms-en.pdf> [*NSG Privacy Breach Protocol*].
[36] *NSG Privacy Breach Protocol*, at p. 15.

[124] The purpose and goal of this type of post-incident review is described as follows in the *NSG Privacy Breach Protocol*:

> Most likely it will be apparent how the breach occurred early in the response process. However, it is important to revisit the root cause of the breach after it has been resolved to ensure the reasons for the breach are well understood and have been rectified.
>
> …
>
> The goal of the investigation is to determine what occurred, identify areas of weakness and what recommendations can be made to prevent a similar situation in the future. These recommendations may take the form of changes to physical, administrative or technical controls, changes to business processes or training and education of employees.[37]

[125] The *Privacy Breach Report*, created by the Nova Scotia Government after the cyberattack, sets out recommendations to itself that I will hereinafter refer to as the *Nova Scotia Government's Post-Incident Recommendations*, as follows:

> MOVEit Secure File Transfer Service
>
> - Apply data access controls for users:
> - Document and manage data access requirements for each use of the MOVEit service, ensuring access requirements align with the stated business purpose.
> - Provide business level descriptions of automated MOVEit tasks. This would decrease the amount of manual work required to assess what data is in each folder should there be system outages.
> - Develop processes or guidelines for appropriate data use:
> - Develop and implement processes or guides to support decision making around data moved through electronic file transfer systems such as MOVEit.
> - Review and confirm retention policies for data stored within the MOVEit system (i.e., MOVEit Transfer folders).
> - Implement additional safeguards for MOVEit and services that use the application:
> - Develop a process to assess the sensitivity of personal information or personal health information to be collected, used, or disclosed within the MOVEit service.
> - Where possible, implement additional security measures such as encryption and password protection for shared files.
> - Implement a second internal (not exposed to the internet) MOVEit instance for files that are shared within government to improve security as it prevents public access to the service.
> - Improve the process of monitoring notices provided by the MOVEit vendor.

[37] *NSG Privacy Breach Protocol*, at p. 15.

- Improve user awareness of the application:
    - Develop and distribute training material, including (FAQs), to business partners on MOVEit, emphasizing an understanding of associated risks and optimal usage.

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. This can include the following key activities:
    - Describe roles and responsibilities of the privacy breach teams to ensure there is clarity in managing various operational aspects during large scale breaches.
    - Design an interdepartmental governance and communication model for large-scale breaches to provide a structured framework that supports decision-making, accountability, and management efforts.
    - Develop a process for reassigning and allocating skilled resources to various workstreams necessary to support a large-scale breach response effort.
    - Review and update the standardized privacy risk assessment tools for large-scale breaches.
    - Review and update templates such as standardized notification letters to assist with timely public notification procedures.
    - Develop and distribute training material, including FAQs, increasing awareness, and understanding of how to respond to large-scale breaches.
- Review and enhance the existing cyber security incident response process. This can include the following key activities:
    - Update the cyber security incident response plan and develop playbooks for common incident scenarios.
    - Conduct mock exercises to enhance the skills and knowledge of the people involved in response efforts to reduce the time needed to technically detect, respond, and contain an incident.
    - Maintain and share in an easy to find manner the current contact information for cyber security incident managers and external security resource supports.
    - Maintain and share in an easy to-find manner, an up-to-date inventory of application information, including appropriate contact details for business owners and responsible support teams.

Data Governance Practices

- Communicate the applicability of existing formalized data classification framework(s) to accurately categorize data based on sensitivity.
- Establish a data retention policy for the government that outlines requirements for data management and disposition throughout the data lifecycle.

[126] The *Privacy Breach Report* states: "the recommendations will require collaboration across departments, public bodies, and other partners such as NSH and IWK. It is intended that those involved assess the recommendations and develop plans for implementation."

[127] I am pleased to see that the *Nova Scotia Government's Post-Incident Recommendations* have been created. The recommendations are comprehensive except in the following ways:

i. Recommendations are permissive. The Nova Scotia Government should be setting out mandatory requirements.
ii. There is no timeline for completion of the tasks (including deadlines) set out in the *Nova Scotia Government's Post-Incident Recommendations*.
iii. The *Nova Scotia Government's Post-Incident Recommendations* state: "the recommendations will require collaboration across departments, public bodies, and other partners such as NSH and IWK. It is intended that those involved assess the recommendations and develop plans for implementation." This wording is not strong enough. Whose role is it to assess the recommendations and implement the plans? Who is accountable if the plans are not implemented? Clear, granular roles must be set out in the recommendations, with final accountability lying at the highest level of government – the Ministerial level.

[128] **Finding #12:** I find that the *Nova Scotia Government's Post-Incident Recommendations* are comprehensive except in the following ways:

i. Recommendations are permissive. The Nova Scotia Government should be setting out mandatory requirements.
ii. There is no timeline for completion of the tasks (including deadlines) set out in the *Nova Scotia Government's Post-Incident Recommendations*.
iii. The *Nova Scotia Government's Post-Incident Recommendations* state: "the recommendations will require collaboration across departments, public bodies, and other partners such as NSH and IWK. It is intended that those involved assess the recommendations and develop plans for implementation." This wording is not strong enough. Whose role is it to assess the recommendations and implement the plans? Who is accountable if the plans are not implemented? Clear, granular roles must be set out in the recommendations, with final accountability lying at the highest level of government – the Ministerial level.

[129] **Recommendation #7:** I recommend that, within 90 days of the date of this report, the Nova Scotia Government complete and post on its website a clear, comprehensive post-incident response plan that:

i. Makes all recommendations set out in the *Nova Scotia Government's Post-Incident Recommendations* mandatory requirements.
ii. Sets out clear timelines and deadlines for completion of all the *Nova Scotia Government's Post-Incident Recommendations* and associated key activities.
iii. Sets out clear accountability at the Ministerial level for implementation of the tasks set out in the post-incident response plan.
iv. Addresses the concerns raised and recommendations made in this report.

[130] **Recommendation #8:** Further to Recommendation #7, I recommend that, within 1 year of the date of this report, the Nova Scotia Government complete the tasks set out in its published post-incident response plan and post the results to its website for the public to view.

5.0 SUMMARY OF FINDINGS AND RECOMMENDATIONS

5.1 Findings

[131] **Finding #1:** I find that a privacy breach occurred.

[132] **Finding #2:** I find that the root cause of the breach was that threat actors exploited a critical vulnerability in the MOVEit file transfer system and used it to gain access to the personal information that was stored in the MOVEit repository.

[133] **Finding #3:** I find that by not conducting a PIA when it began its use of the MOVEit file transfer system or when the Nova Scotia Government's privacy policy was adopted in 2008 and updated in 2018, the Nova Scotia Government failed to have reasonable security and information practices in place and was therefore not in compliance with s. 24(3) of *FOIPOP* or ss. 61, 62 and 65 of *PHIA*.

[134] **Finding #4:** I find that the MOVEit file transfer system was frequently and inappropriately used as a repository for extraneous records and that this exacerbated the extent of the personal information breached in the cyberattack.

[135] **Finding #5:** I find that the Nova Scotia Government did not provide sufficient direction to MOVEit users regarding the length of time that files should be kept in the repository of the MOVEit file transfer system and that this exacerbated the extent of the personal information breached in the cyberattack.

[136] **Finding #6:** I find that the Nova Scotia Government took reasonable steps to contain the privacy breach following its discovery. Specifically, the response was timely and engaged third-party cyber security experts who provided essential instructions.

[137] **Finding #7:** I find that the harm from this privacy breach is significant and was foreseeable.

[138] **Finding #8:** I find that the 5-year credit monitoring offered to affected individuals by the Nova Scotia Government is reasonable.

[139] **Finding #9:** I find that the timing of the indirect and direct privacy breach notification to affected individuals was reasonable.

[140] **Finding #10:** I find that the notification letters and call centre staff provided insufficient information regarding the breach and the personal information impacted.

[141] **Finding #11:** I find the contact information used for the notification letters was severely outdated in many cases. This meant that thousands of affected individuals did not receive notification letters and were unable to take measures to protect themselves.

[142] **Finding #12:** I find that the *Nova Scotia Government's Post-Incident Recommendations* are comprehensive except in the following ways:

i. Recommendations are permissive. The Nova Scotia Government should be setting out mandatory requirements.
ii. There is no timeline for completion of the tasks (including deadlines) set out in the *Nova Scotia Government's Post-Incident Recommendations*.
iii. The *Nova Scotia Government's Post-Incident Recommendations* state: "the recommendations will require collaboration across departments, public bodies, and other partners such as NSH and IWK. It is intended that those involved assess the recommendations and develop plans for implementation." This wording is not strong enough. Whose role is it to assess the recommendations and implement the plans? Who is accountable if the plans are not implemented? Clear, granular roles must be set out in the recommendations, with final accountability lying at the highest level of government – the Ministerial level.

5.2 Recommendations

[143] **Recommendation #1:** In August 2024, the Nova Scotia Government indicated that a PIA for MOVEit was being completed at that time. If this task is not yet finished, I recommend that the Nova Scotia Government complete a thorough and up-to-date PIA on its use of the MOVEit file transfer system within 60 days of the date of this report.

[144] **Recommendation #2:** I further recommend that, within 60 days of the date of this report, the Nova Scotia Government make the appropriate portions of the PIA on MOVEit publicly available on its website. Any portions of the PIA that could provide an opportunity for future exploitation by threat actors should not be reported publicly.

[145] **Recommendation #3:** I recommend that, within 60 days of the date of this report, the Nova Scotia Government create clear retention and disposition schedules for all users of the MOVEit file transfer system that specifies the maximum amount of time that files being transferred can remain in the repository of MOVEit.

[146] **Recommendation #4:** I further recommend that the Nova Scotia Government commit to ensuring that retention and disposition schedules are adhered to by monitoring use of the MOVEit system on a yearly basis, if not more frequently.

[147] **Recommendation #5:** I recommend that, within 60 days of the date of this report, the Nova Scotia Government confirm a commitment to consult with the OIPC in advance of issuing privacy breach notification letters for future major privacy breaches in a manner that allows sufficient time for OIPC suggestions to be incorporated into the notification letters.

[148] **Recommendation #6:** I recommend that the Nova Scotia Government make every reasonable effort to ensure that it has up-to-date contact information for all citizens that it holds personal information about.

[149] **Recommendation #7:** I recommend that, within 90 days of the date of this report, the Nova Scotia Government complete and post on its website a clear, comprehensive post-incident response plan that:

i. Makes all recommendations set out in the *Nova Scotia Government's Post-Incident Recommendations* mandatory requirements.
ii. Sets out clear timelines and deadlines for completion of all the *Nova Scotia Government's Post-Incident Recommendations* and associated key activities.
iii. Sets out clear accountability at the Ministerial level for implementation of the tasks set out in the post-incident response plan.
iv. Addresses the concerns raised and recommendations made in this report.

[150] **Recommendation #8:** Further to Recommendation #7, I recommend that, within 1 year of the date of this report, the Nova Scotia Government complete the tasks set out in its published post-incident response plan and post the results to its website for the public to view.

6.0 ACKNOWLEDGEMENTS

[151] I would like to thank the many people who cooperated with this investigation from the Nova Scotia Government, as well as NSH and IWK Health. The purpose of these investigation reports is to ensure that lessons to be learned from a privacy breach are shared for the benefit of Nova Scotians and for the education of all.

[152] I would also like to thank Jason Mighton, Senior Investigator with the OIPC, who led this investigation and the drafting of this report. I am grateful to Sarah Gallant, Director of Investigations with the OIPC, who assisted in the early stages of this investigation.

[153] Finally, I would like to express my sincere thanks and appreciation to all OIPC staff. My team stepped up to the plate and successfully handled the influx of calls and complaints from those affected by the MOVEit breach. Nova Scotians should be thankful to the OIPC staff for their continued diligence in ensuring that their privacy rights are protected.

February 19, 2025

Tricia Ralph
Information and Privacy Commissioner for Nova Scotia